COMTREND CORPORATION

AR-5382u

ADSL2+ WLAN Router

User Manual

Version A1.0, June 11, 2010

261056-049

Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix C - Specifications

Copyright

Copyright© 2010 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

NOTE:	This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

Table of Contents

CHAPTER 1 INTRODUCTION 5
1.1 FEATURES 5
1.2 APPLICATION 6

CHAPTER 2 INSTALLATION 7
2.1 HARDWARE SETUP 7
2.2 LED INDICATORS 10

CHAPTER 3 WEB USER INTERFACE 12
3.1 DEFAULT SETTINGS 12
3.2 IP CONFIGURATION 12
3.3 LOGIN PROCEDURE 15

CHAPTER 4 DEVICE INFORMATION 17
4.1 WAN 18
4.2 STATISTICS 19
4.2.1 LAN Statistics 19
4.2.2 WAN Statistics 20
4.2.3 xTM Statistics 21
4.2.4 xDSL Statistics 22
4.3 ROUTE 26
4.4 ARP 27
4.5 DHCP 28

CHAPTER 5 ADVANCED SETUP 29
5.1 LAYER 2 INTERFACE 30
5.1.1 ATM Interface 30
5.1.2 PTM Interface 31
5.2 WAN SERVICE 32
5.3 LAN 33
5.4 NAT 35
5.4.1 Virtual Servers 35
5.4.2 Port Triggering 36
5.4.3 DMZ Host 38
5.5 SECURITY 39
5.5.1 IP Filtering 39
5.5.2 MAC Filtering 41
5.6 PARENTAL CONTROL 43
5.6.1 Time Restriction 43
5.6.2 URL Filter 44
5.7 QUALITY OF SERVICE (QOS) 45
5.7.1 Queue Management Configuration 45
5.7.2 Queue Configuration 46
5.7.3 QoS Classification 47
5.8 ROUTING 49
5.8.1 Default Gateway 49
5.8.2 Static Route 49
5.8.3 RIP 50
5.9 DNS 51
5.9.1 DNS Server 51
5.9.2 Dynamic DNS 52
5.10 DSL 53
5.11 UPNP 55
5.12 DNS PROXY 56
5.13 PRINT SERVER 57
5.14 INTERFACE GROUPING 57
5.15 IPSEC 59
5.16 CERTIFICATE 62
5.16.1 Local 62

5.16.2 Trusted CA *64*
5.17 MULTICAST 66

CHAPTER 6 WIRELESS 67
6.1 BASIC 67
6.2 SECURITY 69
6.2.1 WPS *71*
6.3 MAC FILTER 76
6.4 WIRELESS BRIDGE 77
6.5 ADVANCED 78
6.6 STATION INFO 81

CHAPTER 7 DIAGNOSTICS 82

CHAPTER 8 MANAGEMENT 83
8.1 SETTINGS 83
8.1.1 Backup Settings *83*
8.1.2 Update Settings *83*
8.1.3 Restore Default *84*
8.2 SYSTEM LOG 85
8.3 TR-069 CLIENT 87
8.4 INTERNET TIME 88
8.5 ACCESS CONTROL 89
8.5.1 Passwords *89*
8.6 UPDATE SOFTWARE 90
8.7 REBOOT 91

APPENDIX A - FIREWALL 92

APPENDIX B - PIN ASSIGNMENTS 95

APPENDIX C - SPECIFICATIONS 96

APPENDIX D - WPS EXTERNAL REGISTRAR 98

APPENDIX E - PRINTER SERVER 101

APPENDIX F - CONNECTION SETUP 107

Chapter 1 Introduction

The AR-5382u is an 802.11n (300Mbps) Wireless ADSL2+ router.
AR-5382u has four 10/100 Base-T Ethernet ports, a Wi-Fi Protected Setup (WPS) button and a Wi-Fi switch button, one USB Host, which can support 3G USB dongle, and is backward compatible with existing 802.11b (11Mbps) and 11g (54Mbps) equipment.

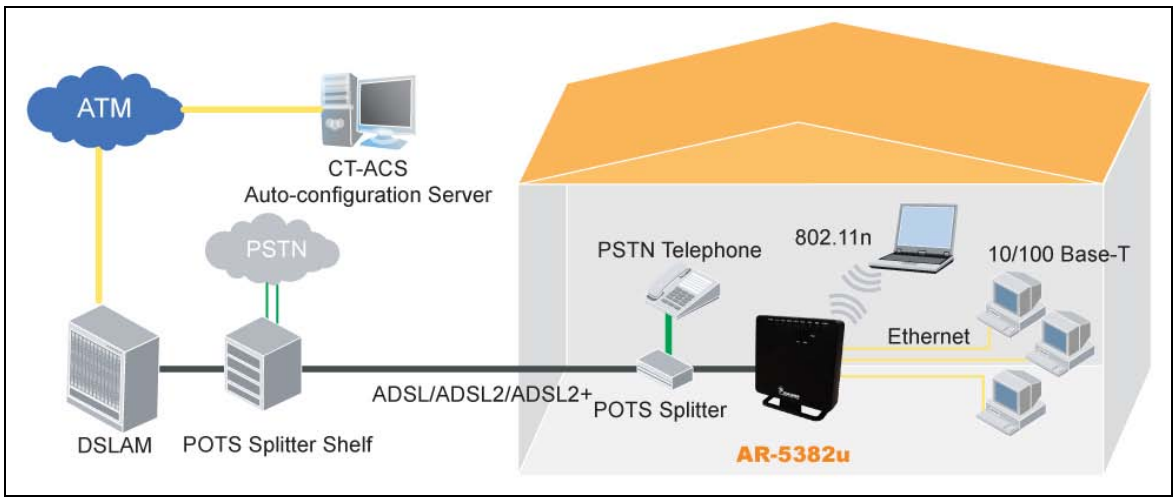
The AR-5382u ADSL2+ router also provides state of the art security features such as 64/128 bit WEP encryption and WPA/WPA2 encryption, Firewall, and VPN pass through. The AR-5382u supports up to 16 contiguous virtual connections allowing for multiple simultaneous Internet connections. The AR-5382u is also designed with TR-068 compliant color panel, which eases the installation of the modem and makes it more user-friendly.

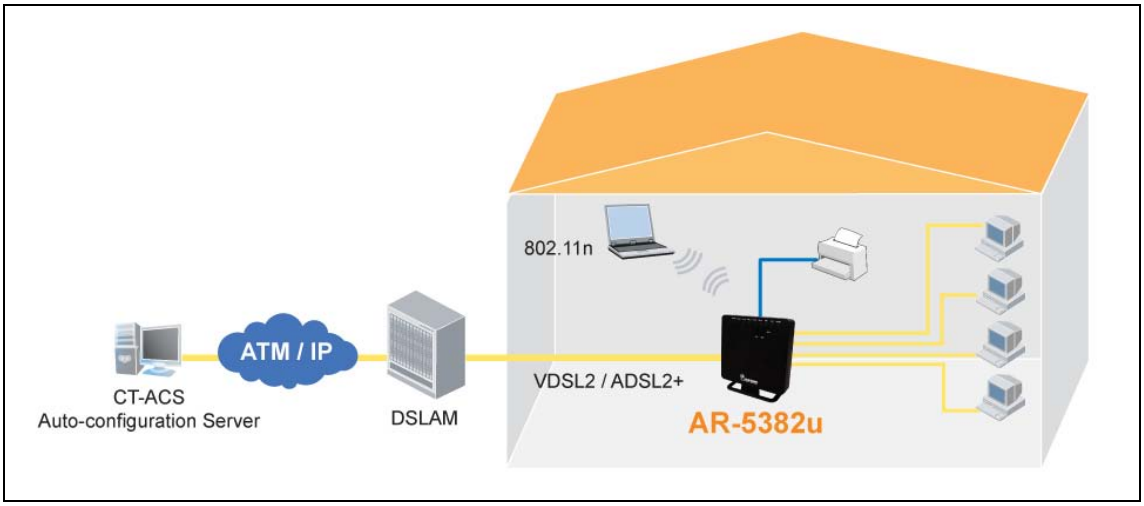
1.1 Features

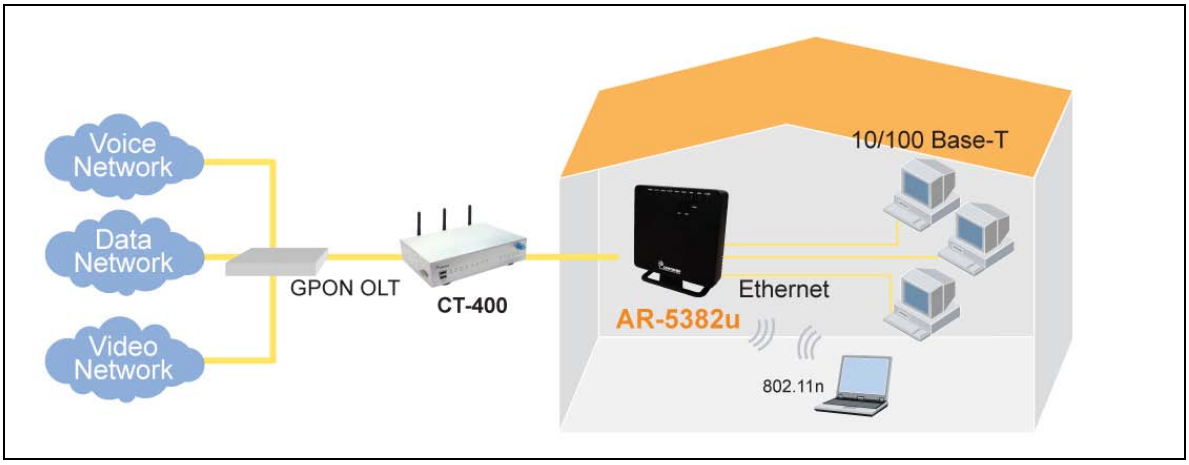
- AR-5382u (Annex A)
- UPnP
- 2x2 MIMO wireless system
- Integrated 802.11n AP (Backward compatible with 802.11b/g)
- WPA/WPA2 and 802.1x
- Wi-Fi Protected Setup (WPS)
- Wireless Distribution System (WDS) support
- WMM
- RADIUS client
- IP/MAC address filtering
- Static route/RIP/RIP v2 routing functions
- Dynamic IP assignment
- IP QoS
- IGMP Proxy
- DHCP Server/Relay/Client
- DNS Proxy
- Auto PVC configuration
- Supports remote administration, automatic firmware upgrade and configuration
- Per-VC packet level QoS
- Up to 16 VCs
- Embedded SNMP agent
- Web-based management
- Configuration backup and restoration FTP/TFTP server
- TR-068 compliant
- NAT/PAT
- Supports TR-069/TR-098/TR-111 for remote management

1.2 Application

The following diagrams depict typical applications of the AR-5382u.



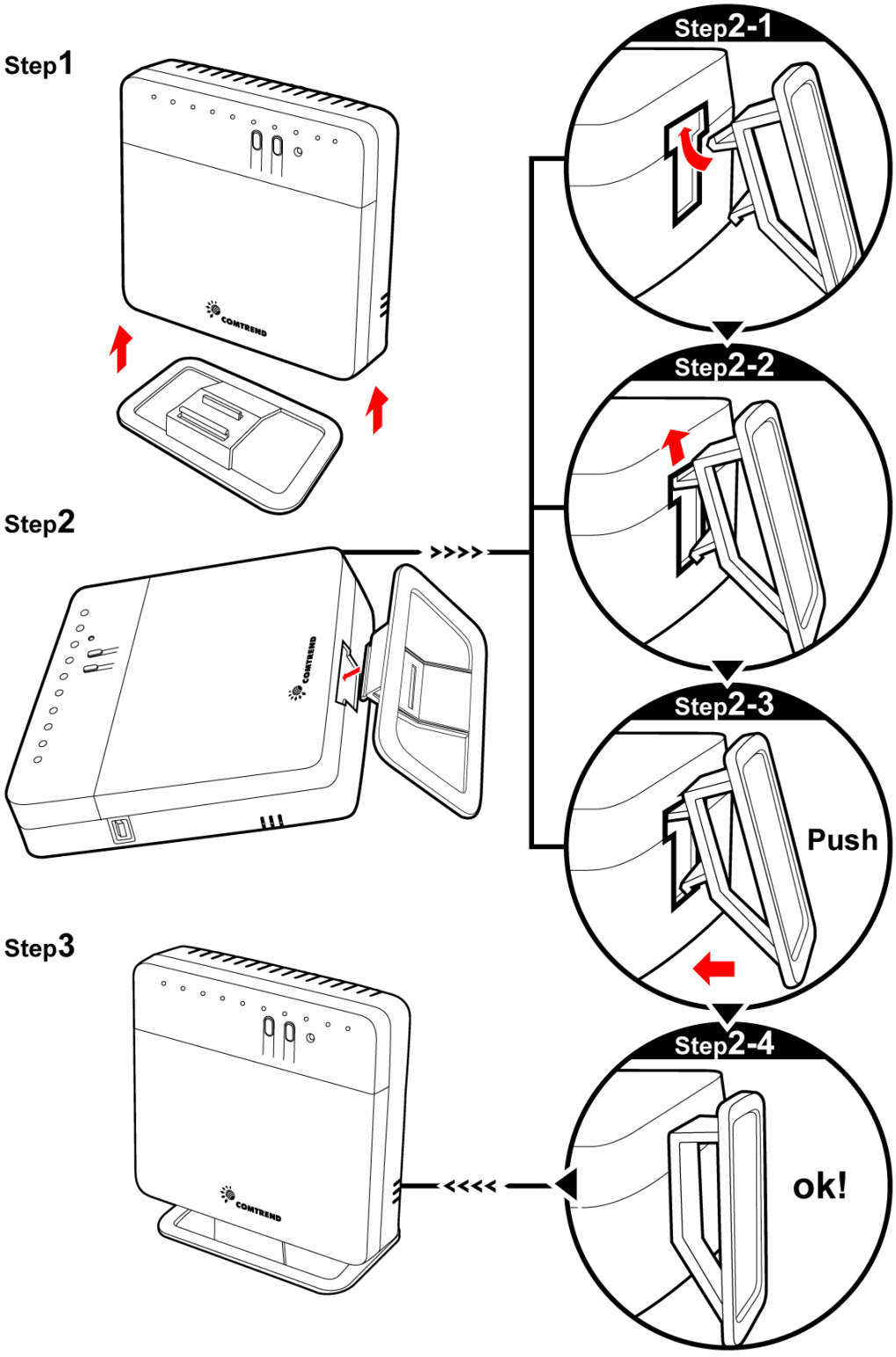




Chapter 2 Installation

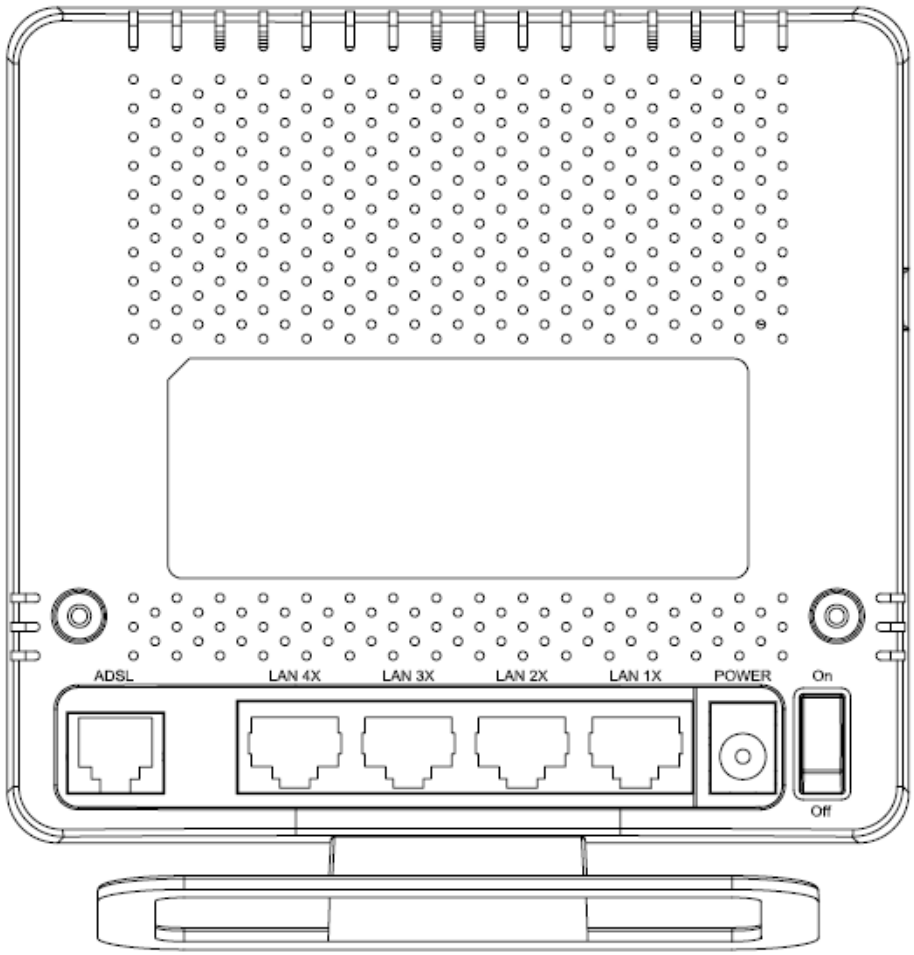
2.1 Hardware Setup

BASE STAND ATTACHMENT



BACK PANEL

The figure below shows the back panel of the device.



ADSL
Connect to the ADSL port with the ADSL RJ11 cable.

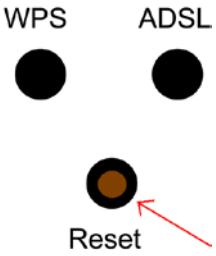
LAN (Ethernet) Ports
You can connect the router to up to four LAN devices using RJ45 cables. The ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

Power ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section 2.2 LED Indicators).

Caution 1:	If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.
Caution 2:	Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

USB Host Port (Type A)
This port can be used to connect the router to the print server.

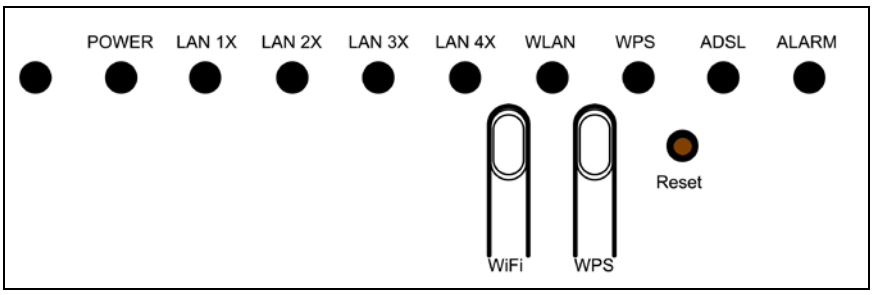
Reset Button
Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.2 LED Indicators for details).



NOTE:	If pressed down for more than 20 seconds, the AR-5382u will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

2.2 LED Indicators

The front panel LED indicators are shown below and explained in the following table. This information can be used to check the status of the device and its connections.



LED	*Color*	*Mode*	*Description*
POWER	Green	On	Power on
		Off	Power off
LAN 1x~4x	Green	On	Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
		Off	No activity, modem power off, no cable or no powered device connected to the associated port
		Blink	LAN activity present (traffic in either direction)
WLAN	Green	On	WiFi is enabled
		Blink	Data transmitting or receiving over WLAN (secured network)
		Off	The wireless module is not installed.
WPS	Green	On	WPS mode exists protected clients
		Blink	WPS mode is on for 120 seconds
		Off	WPS mode is off
ADSL	Green	On	The ADSL link is established.
		Off	The ADSL link is not established.
		Blink	The ADSL link is training.
Alarm	Red	On	The ADSL link is terminated.
		Off	Normal operating status.

WiFi Button
Press to start the wireless function. Press again to terminate the wireless function.

WPS Button
Press to start the WPS function. (See LED description above). Press again to terminate the WPS function.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root** , password: **12345**)
- User access (username: **user**, password: **user**)
- Remote (WAN) access (username: **support**, password: **support**)
- WLAN access: **enabled**

Technical Note

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 IP Configuration

DHCP MODE

When the AR-5382u powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

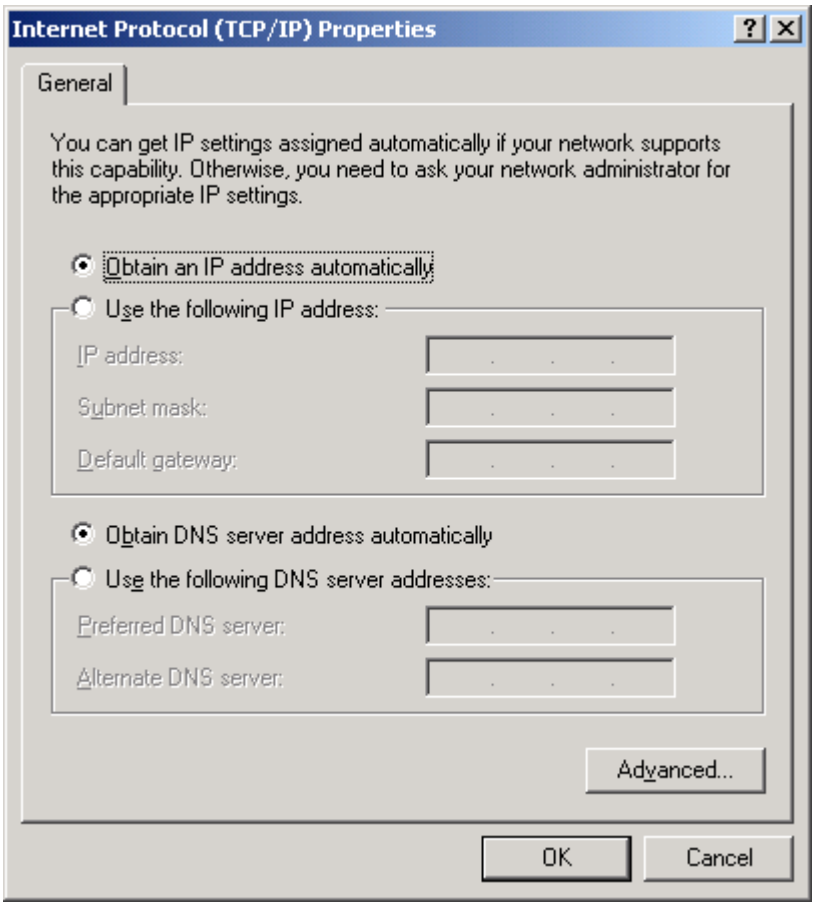
To obtain an IP address from the DCHP server, follow the steps provided below.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Select Obtain an IP address automatically as shown below.



STEP 4: Click **OK** to submit these settings.

If you experience difficulty with DHCP mode, you can try static IP mode instead.

STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

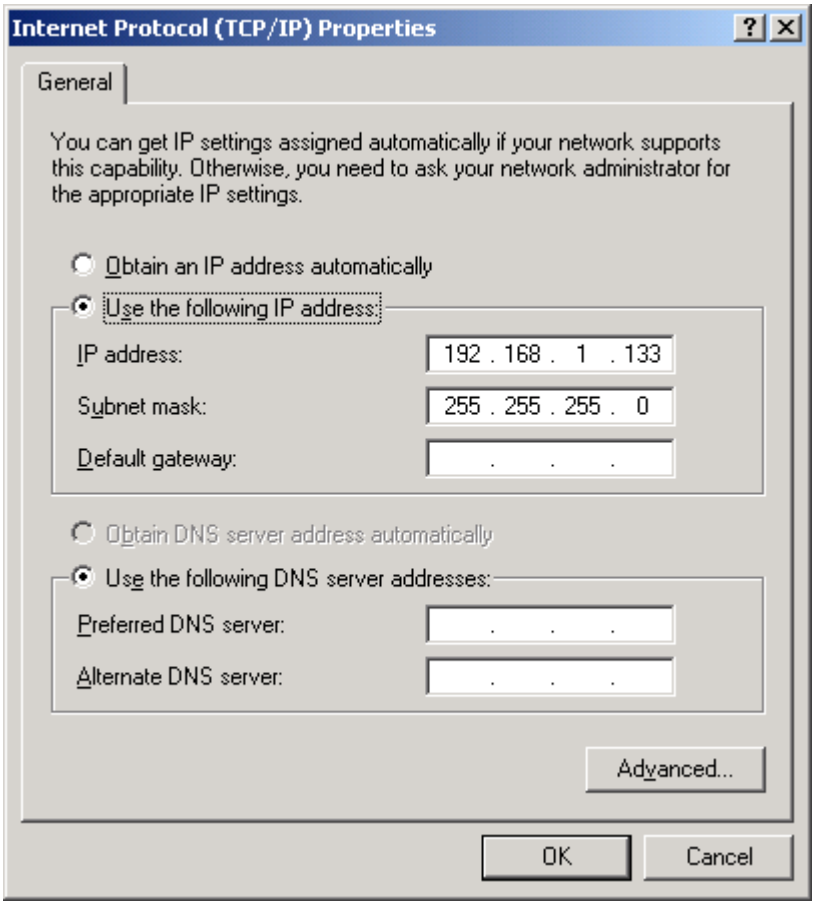
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



STEP 4: Click **OK** to submit these settings.

3.3 Login Procedure

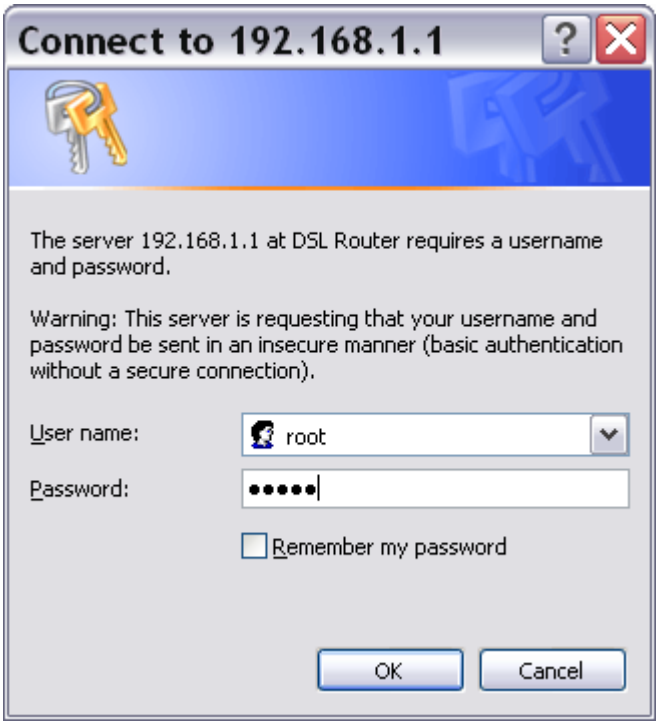
Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in 3.1 Default Settings.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Chapter 4 Device Information screen and login with remote username and password.

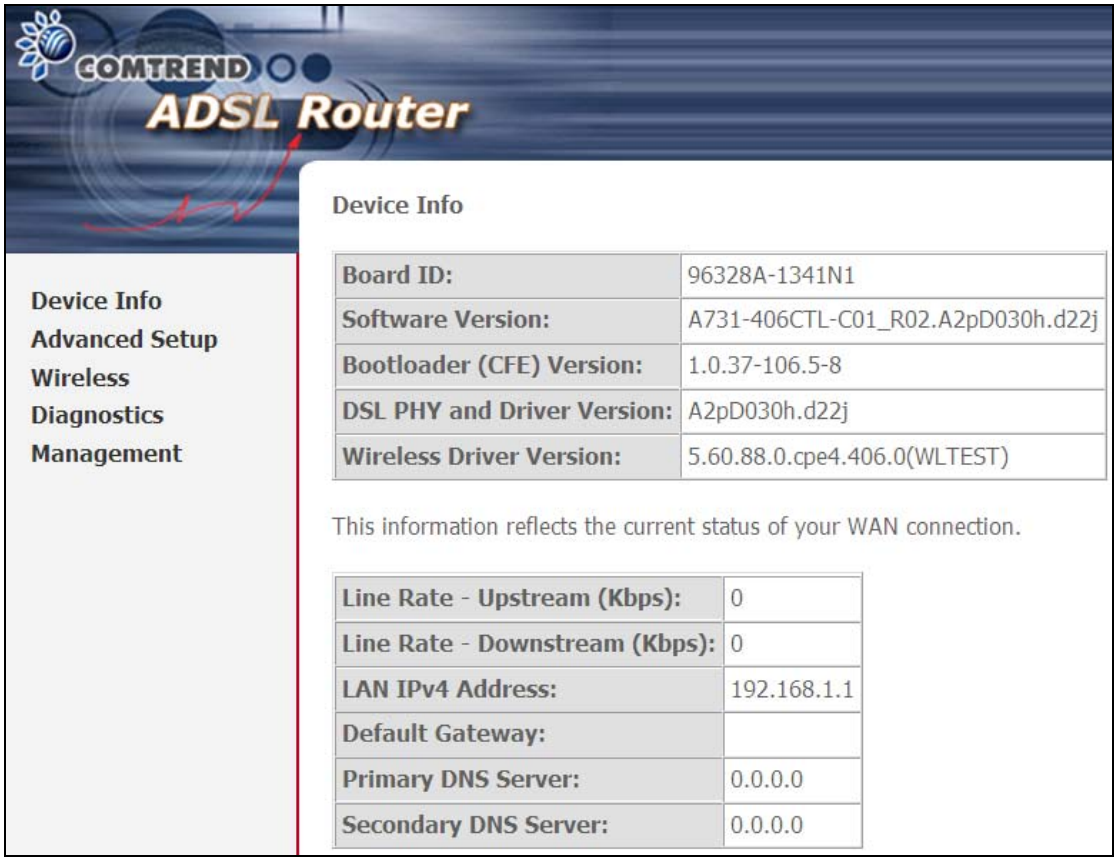
STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.



Click **OK** to continue.

NOTE:	The login password can be changed later (see 8.5.1 Passwords).

STEP 3: After successfully logging in for the first time, you will reach this screen.



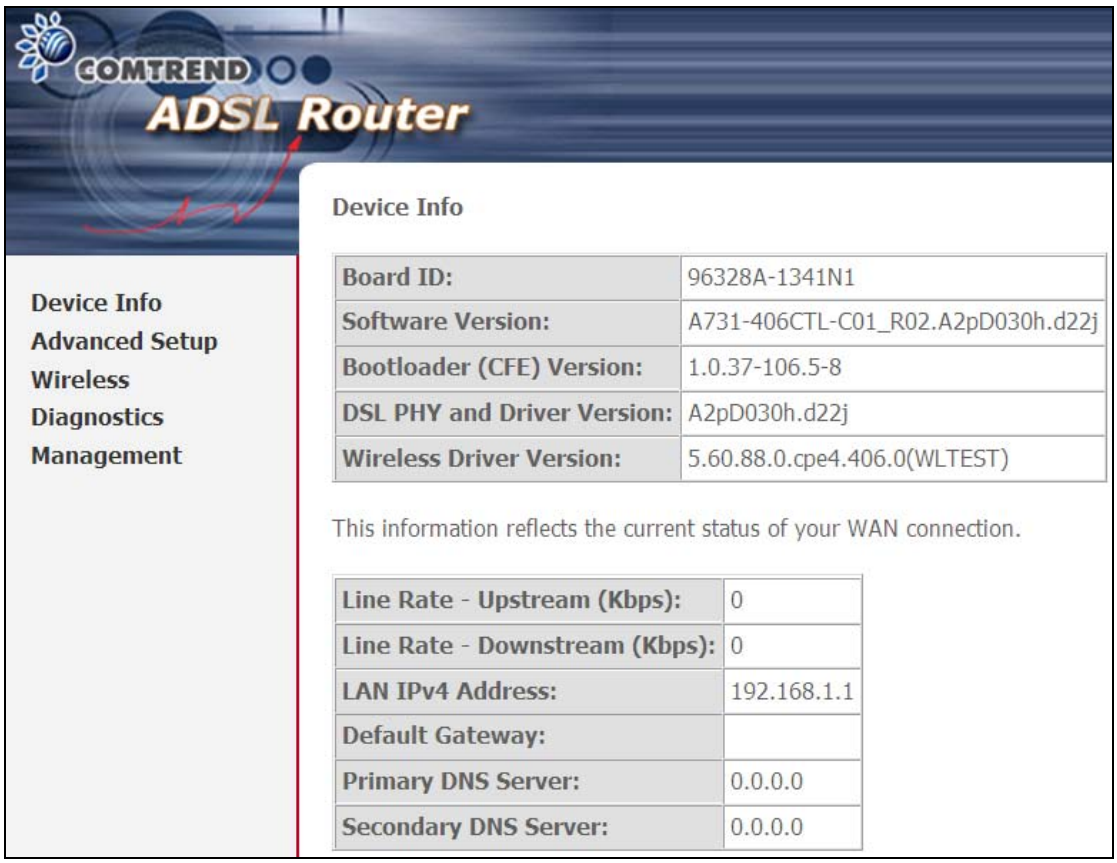
Chapter 4 Device Information

The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

NOTE:	The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

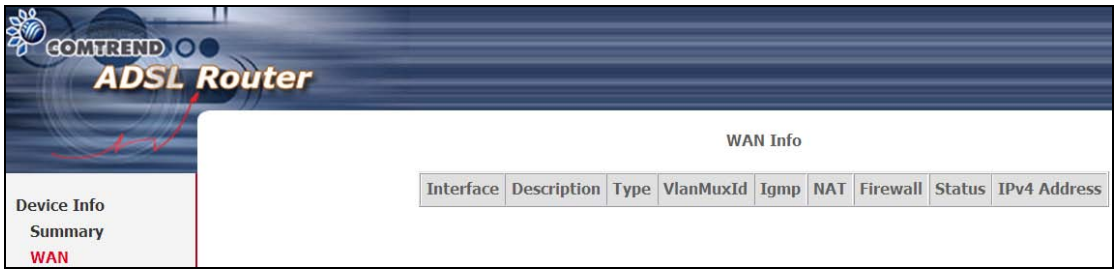
The Device Info Summary screen displays at startup.



This screen shows hardware, software, IP settings and other related information.

4.1 WAN

Select WAN from the Device Info submenu to display the configured PVC(s).



Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address

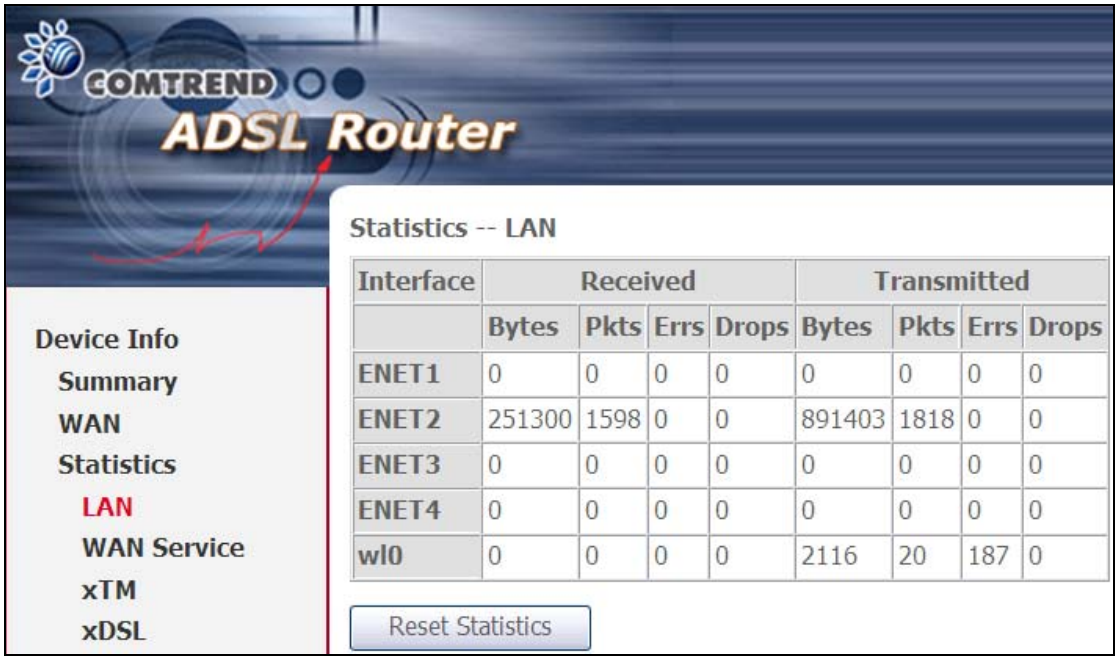
4.2 Statistics

This selection provides LAN, WAN, ATM/PTM and xDSL statistics.

NOTE:	These screens are updated automatically every 15 seconds. Click **Reset Statistics** to perform a manual update.

4.2.1 LAN Statistics

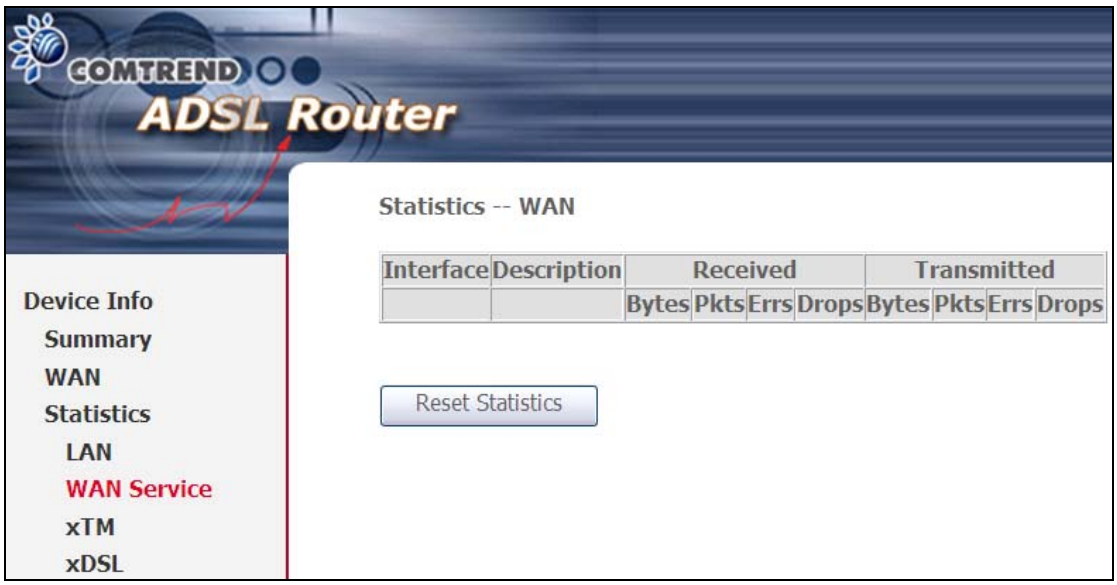
This screen shows data traffic statistics for each LAN interface.



Heading		Description
Interface		LAN interface(s)
Received/Transmitted:	- Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.2 WAN Statistics

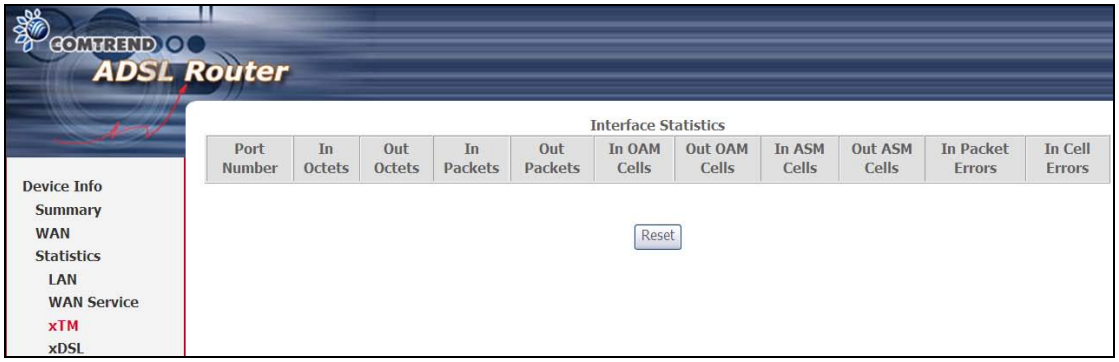
This screen shows data traffic statistics for each WAN interface.



Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.3 xTM Statistics

The following figure shows Asynchronous Transfer Mode (xTM) statistics.

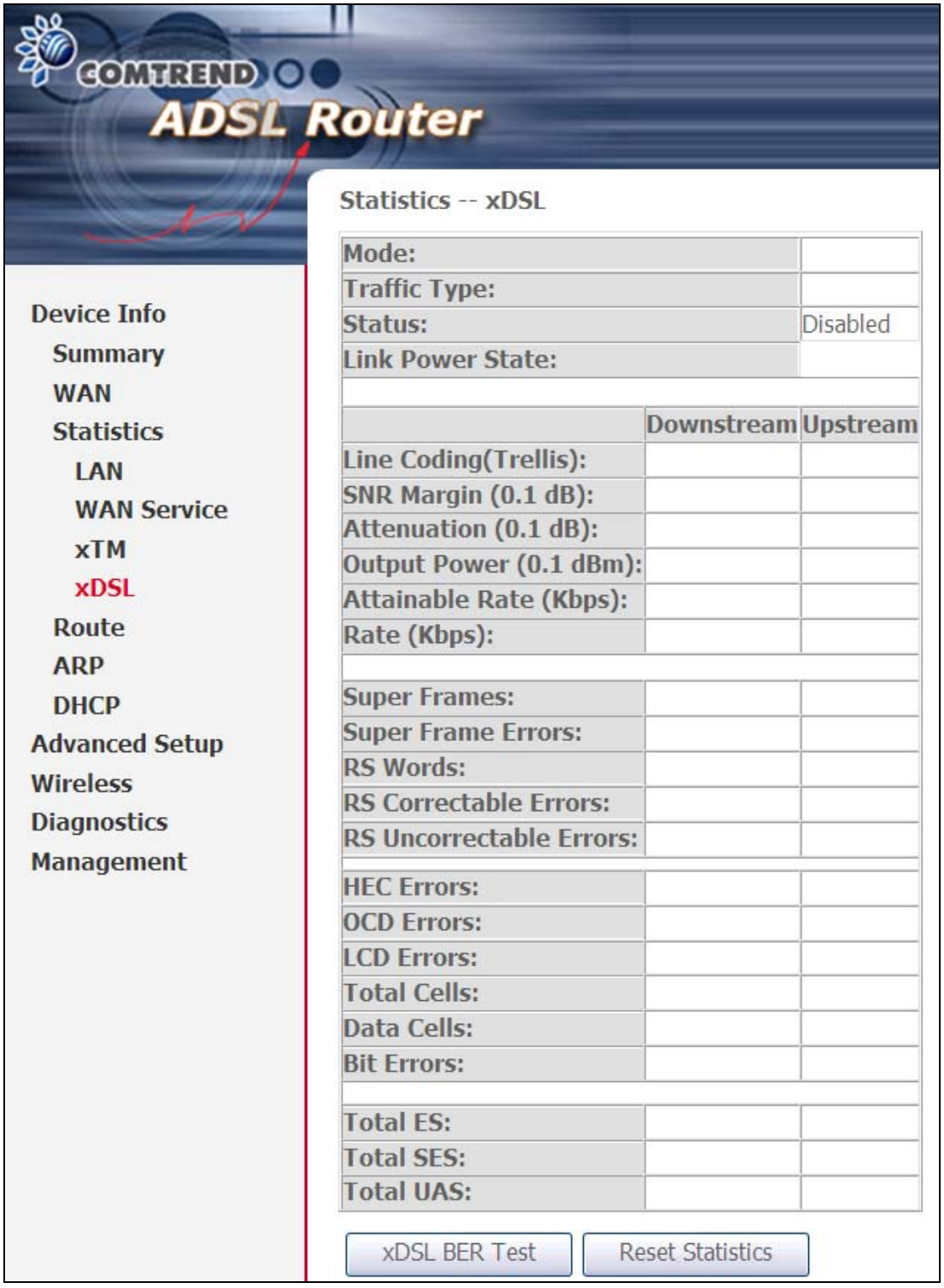


ATM Interface Statistics

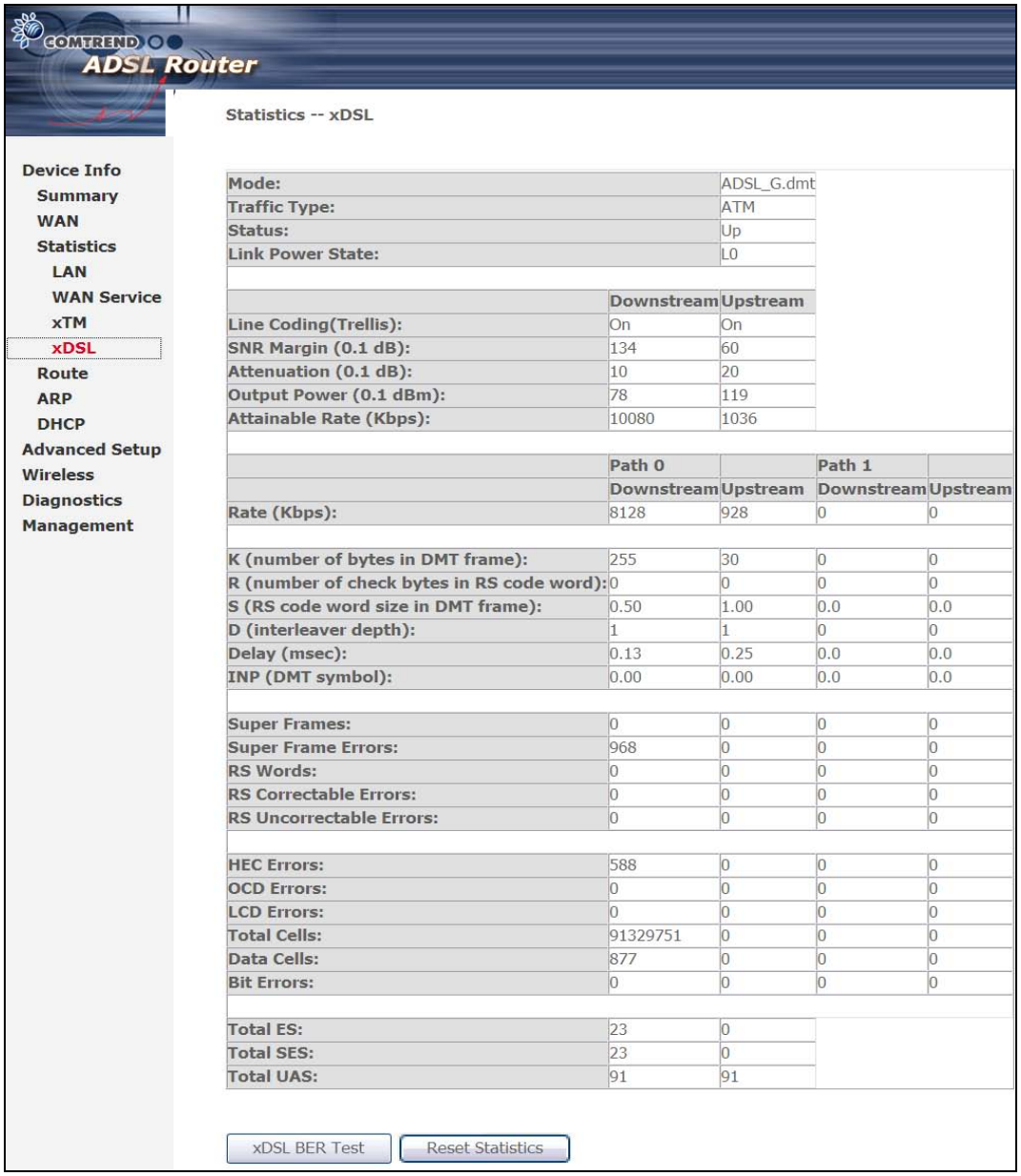
Heading	Description
Port Number	ATM PORT (0-3)
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEC error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

4.2.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type.



The **ADSL** example is shown here.



Click the **Reset Statistics** button to refresh this screen.

Field	Description
Mode	G.Dmt, G.lite, T1.413, ADSL2, ADSL2+,VDSL, VDSL2
Traffic Type	Channel type Interleave or Fast
Status	Lists the status of the DSL link
Link Power State	Link output power state.

Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction.

Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rates downstream/upstream

In VDSL mode, the following section is inserted.

B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in a RS codeword
T	Number of Mux Data Frames in an OH sub-frame
R	Number of redundancy bytes in the RS codeword
S	Number of data symbols the RS codeword spans
L	Number of bits transmitted in each data symbol
D	The interleaver depth
I	The interleaver block size in bytes
N	RS codeword size
Delay	The delay in milliseconds (msec)
INP	DMT symbol

In ADSL2+ mode, the following section is inserted.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Mux Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)
INP	DMT symbol

In G.DMT mode, the following section is inserted.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors

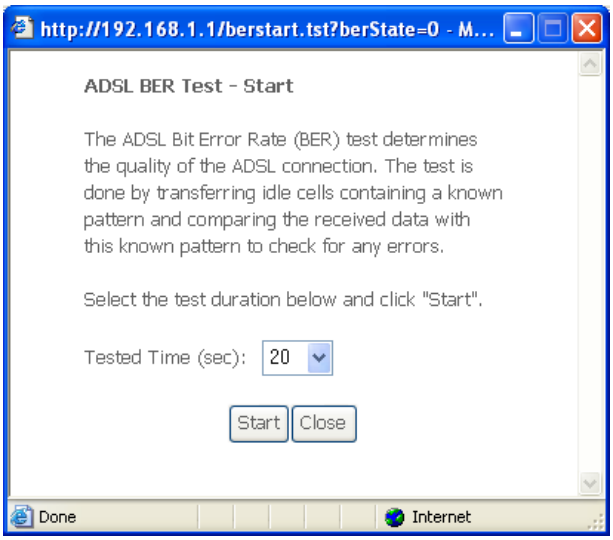
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

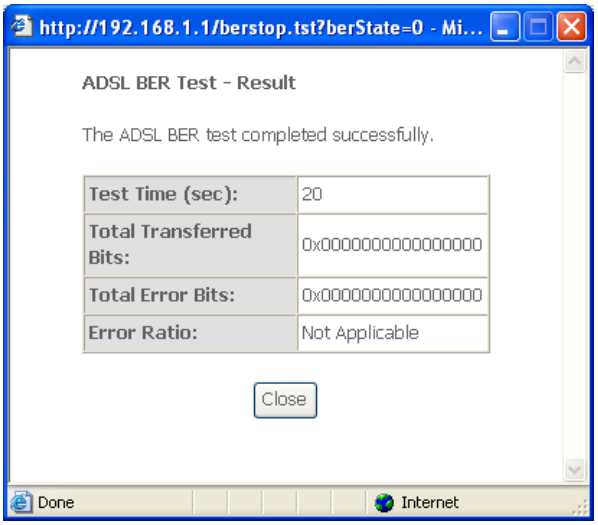
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

xDSL BER TEST

Click **xDSL BER Test** on the xDSL Statistics screen to test the Bit Error Rate (BER). A small pop-up window will open after the button is pressed, as shown below.

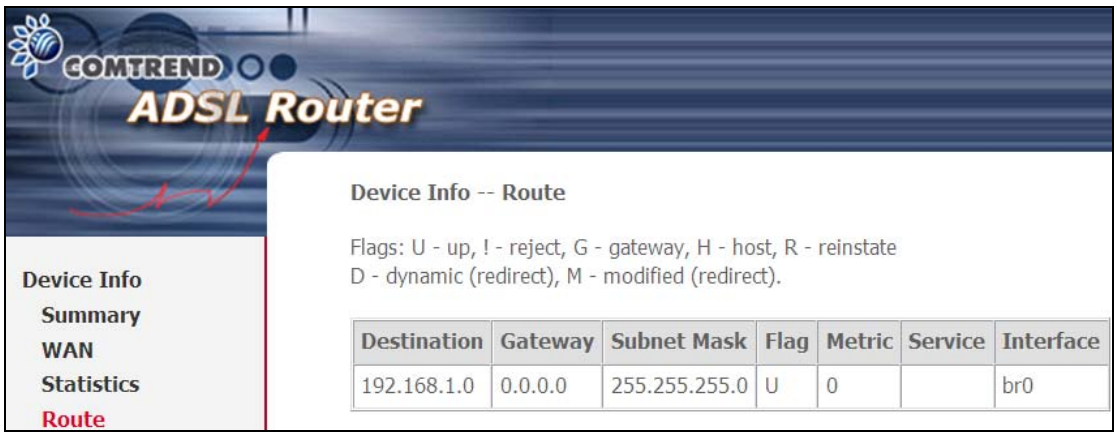


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



4.3 Route

Choose **Route** to display the routes that the AR-5382u has found.



Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

4.4 ARP

Click **ARP** to display the ARP information.

Field	Description
IP address	Shows IP address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

4.5 DHCP

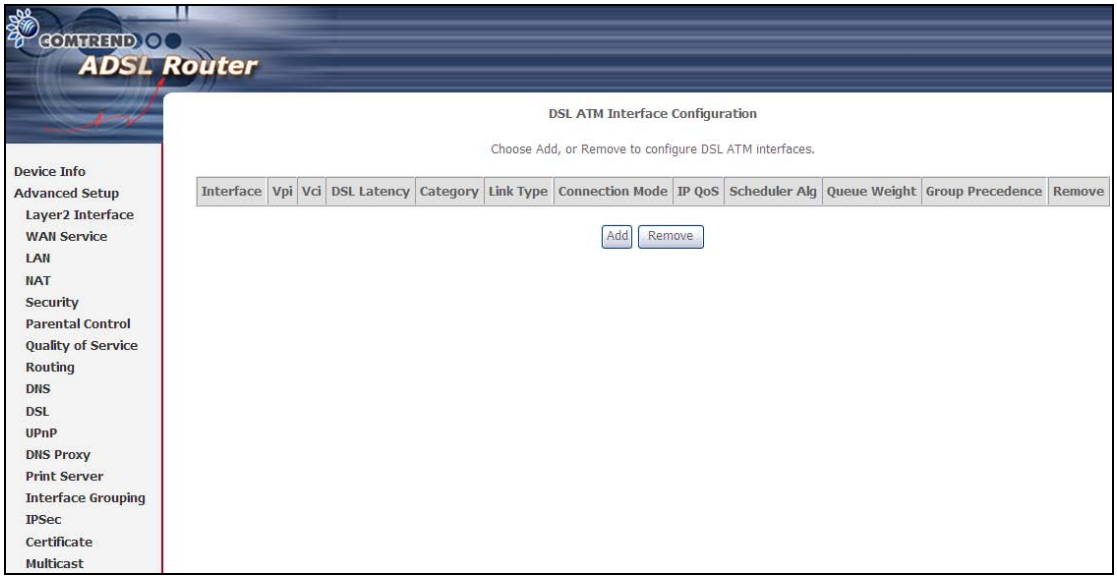
Click **DHCP** to display all DHCP Leases.

Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

Chapter 5 Advanced Setup

Click on the link to jump to a specific section:

5.1 Layer 2 Interface
5.2 WAN Service
5.3 LAN
5.4 NAT
5.5 Security
5.6 Parental Control
5.7 Quality of Service (QoS)
5.8 Routing
5.9 DNS
5.10 DSL
5.11 UPnP
5.12 DNS Proxy
5.13 Print Server
5.14 Interface Grouping
5.15 IPSec
5.16 Certificate
5.17 Multicast



5.1 Layer 2 Interface

The ATM interface screen is described here.

5.1.1 ATM Interface

Add or remove ATM interface connections here.

Click **Add** to create a new ATM interface (see Appendix F - Connection Setup).

NOTE:	Up to 8 ATM interfaces can be created and saved in flash memory.

To remove a connection, select its Remove column radio button and click **Remove**.

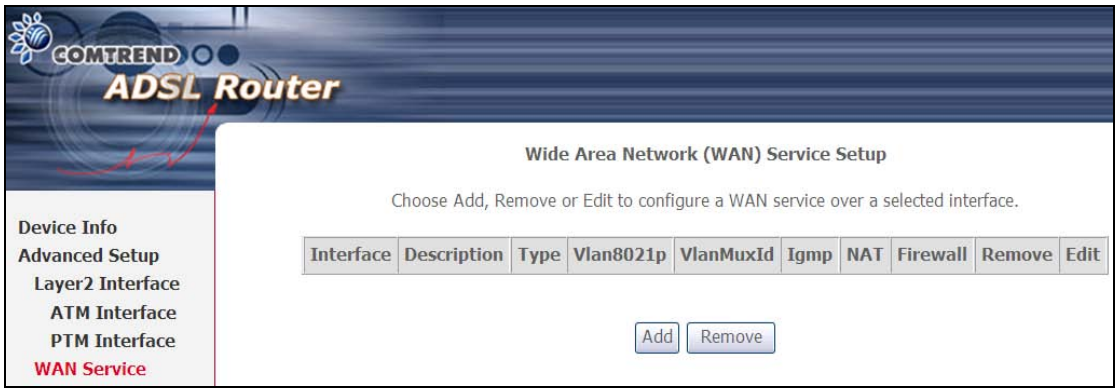
5.1.2 PTM Interface

Add or remove PTM interface connections here.

Click **Add** to create a new connection (see Appendix F - Connection Setup). To remove a connection, select its Remove column radio button and click **Remove**.

5.2 WAN Service

This screen allows for the configuration of WAN interfaces.



Click the **Add** button to create a new connection. For connections on ATM or PTM WAN interfaces see Appendix F - Connection Setup.

NOTE:	ATM and PTM service connections cannot coexist. In Default Mode, up to 8 WAN connections can be configured; while VLAN Mux and MSC Connection Modes support up to 16 WAN connections.

To remove a connection, select its Remove column radio button and click **Remove.**

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
Remove	Select interfaces to remove
Edit	Select interfaces to edit

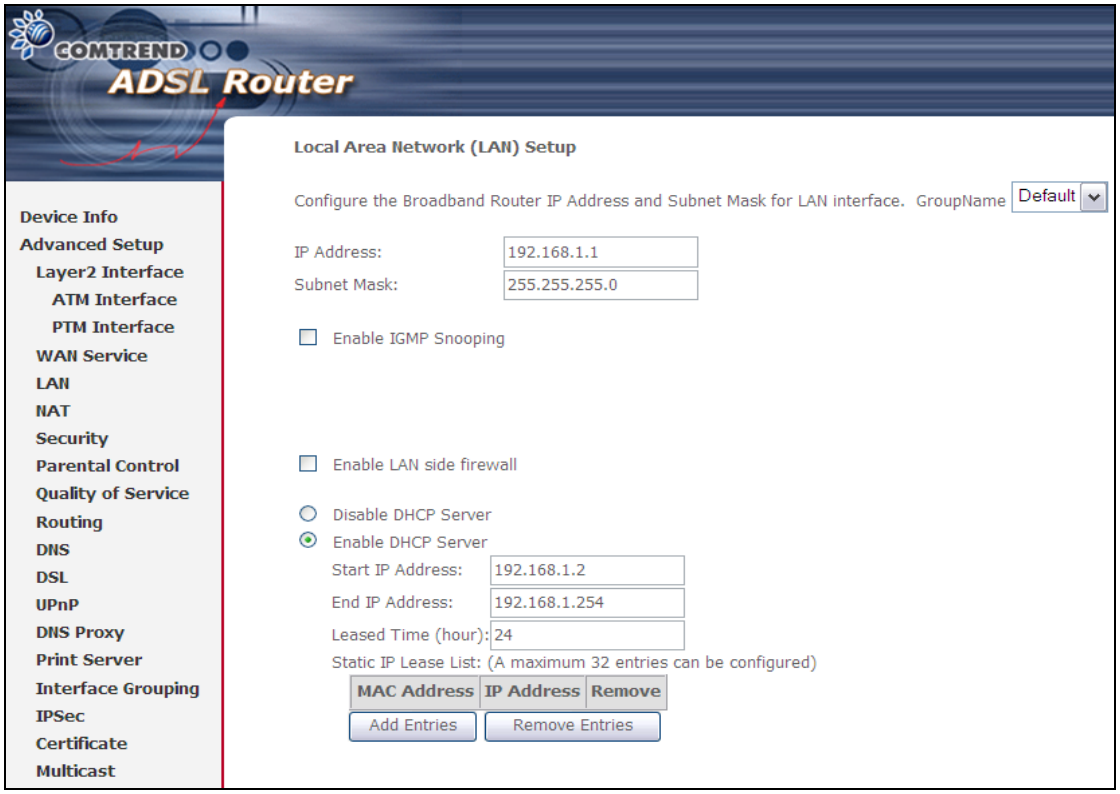
To remove a connection, select its Remove column radio button and click **Remove.**

To **Add** a new WAN connection, click the **Add** button and follow the instructions.

NOTE:	Up to 16 PVC profiles can be configured and saved in flash memory. Also, ATM and PTM service connections cannot coexist.

5.3 LAN

Configure the LAN interface settings and then click **Apply / Save**.



Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable IGMP Snooping: Enable by ticking the checkbox ☑.

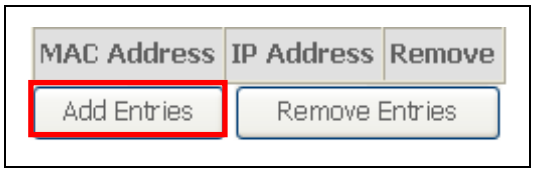
Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

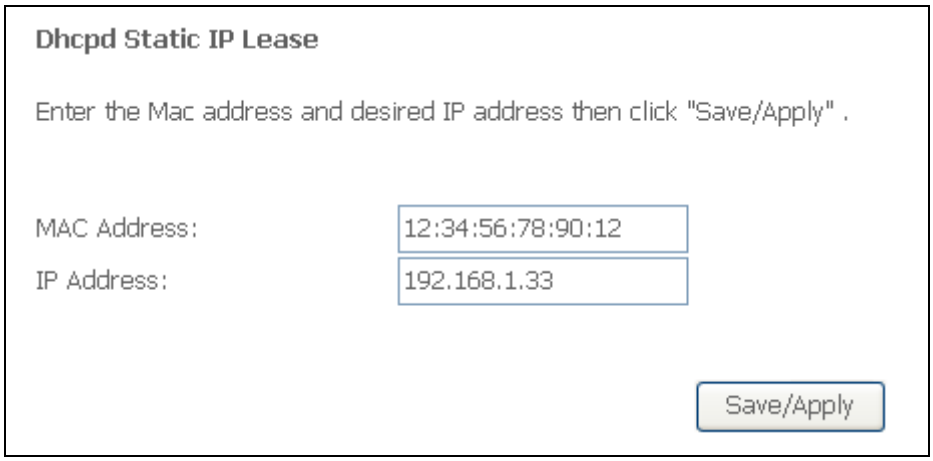
Enable LAN side firewall: Enable by ticking the checkbox ☑.

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Static IP Lease List: A maximum of 32 entries can be configured.



To add an entry, enter MAC address and Static IP and then click **Save / Apply**.

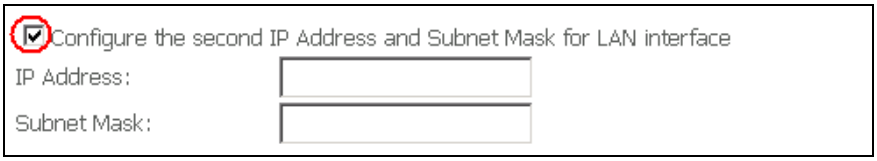


To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.

DHCP Server Relay: Enable with checkbox ☑ and enter DHCP Server IP address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address. ***This option is hidden if NAT is enabled or when the router is configured with only one Bridge PVC.***

2ND LAN INTERFACE

To configure a secondary IP address, tick the checkbox ☑ outlined (in RED) below.



IP Address: Enter the secondary IP address for the LAN port.

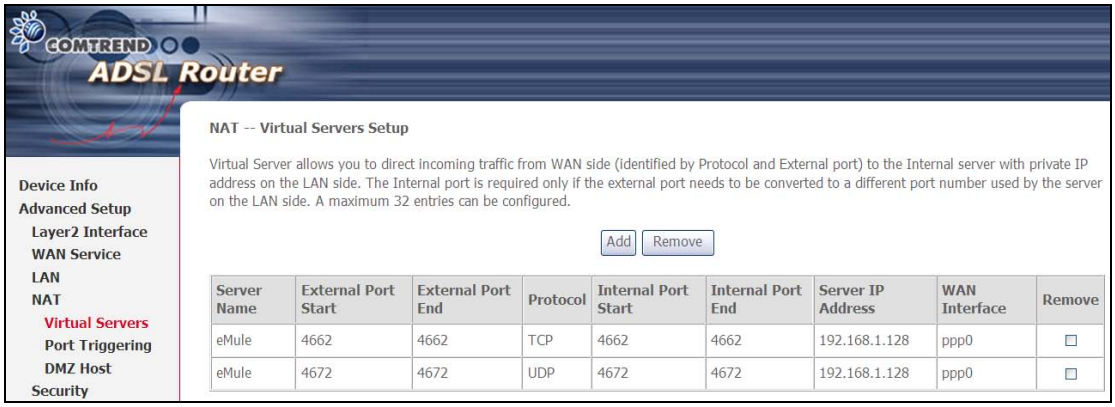
Subnet Mask: Enter the secondary subnet mask for the LAN port.

5.4 NAT

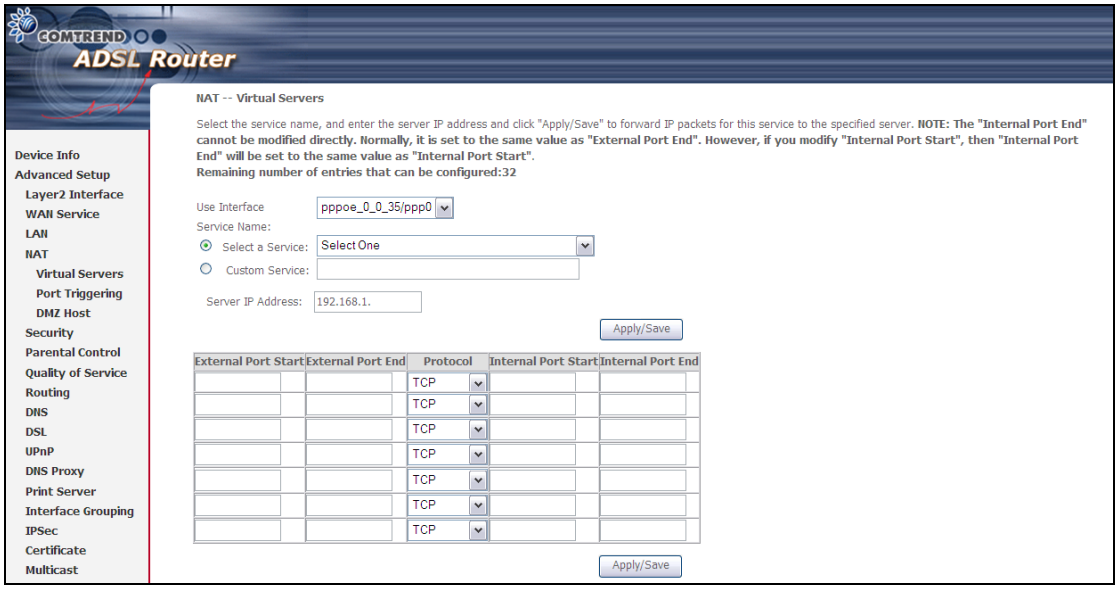
To display this option, NAT must be enabled in at least one PVC shown on the Chapter 5 Advanced Setup - . *NAT is not an available option in Bridge mode*.

5.4.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
A maximum of 32 entries can be configured.



To add a Virtual Server, click **Add**. The following will be displayed.



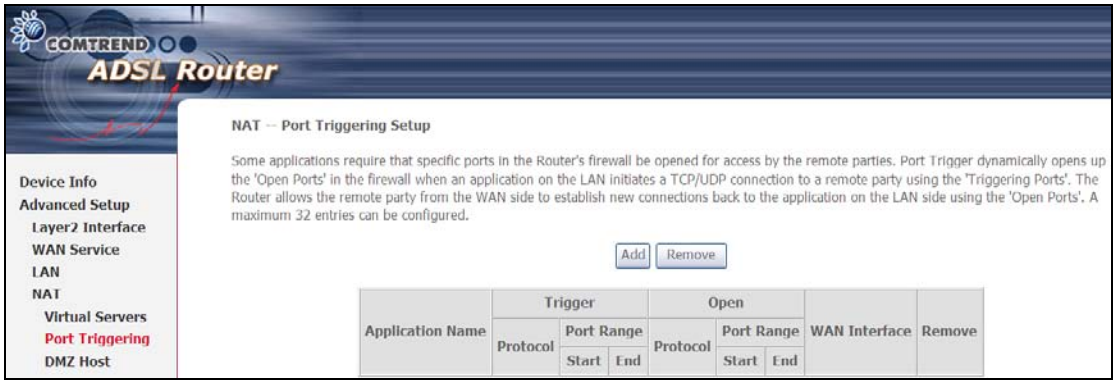
Consult the table below for field and header descriptions.

Field / Header	Description
Use Interface	Select a WAN interface from the drop-down box.

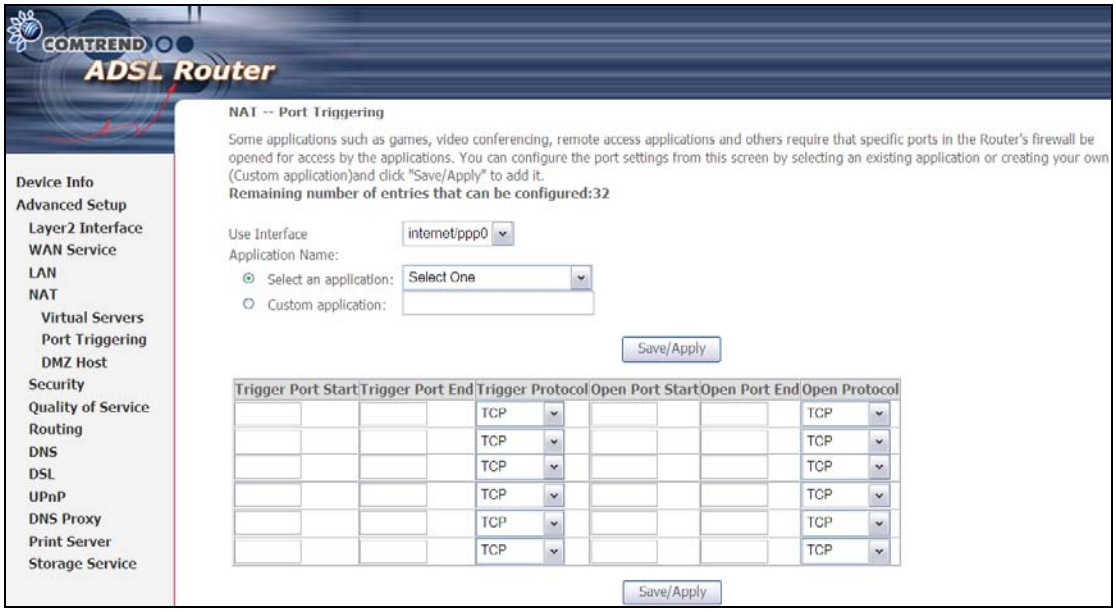
Field / Header	Description
Select a Service **Or** Custom Service	User should select the service from the list. **Or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

5.4.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



To add a Trigger Port, click **Add**. The following will be displayed.

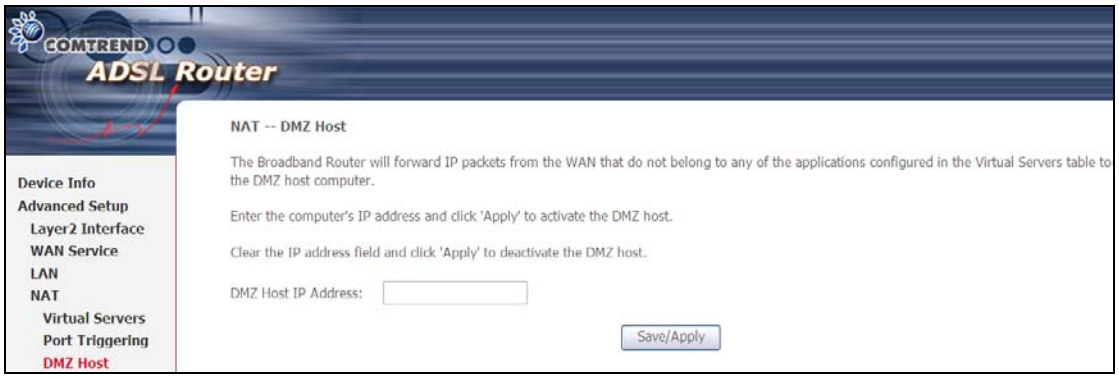


Consult the table below for field and header descriptions.

Field / Header	Description
Use Interface	Select a WAN interface from the drop-down box.
Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP, or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP, or UDP.

5.4.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



To **Activate** the DMZ host, enter the DMZ host IP address and click **Save / Apply**.

To **Deactivate** the DMZ host, clear the IP address field and click **Save / Apply**.

5.5 Security

To display this function, you must enable the firewall feature in WAN Setup.
For detailed descriptions, with examples, please consult Appendix A - Firewall

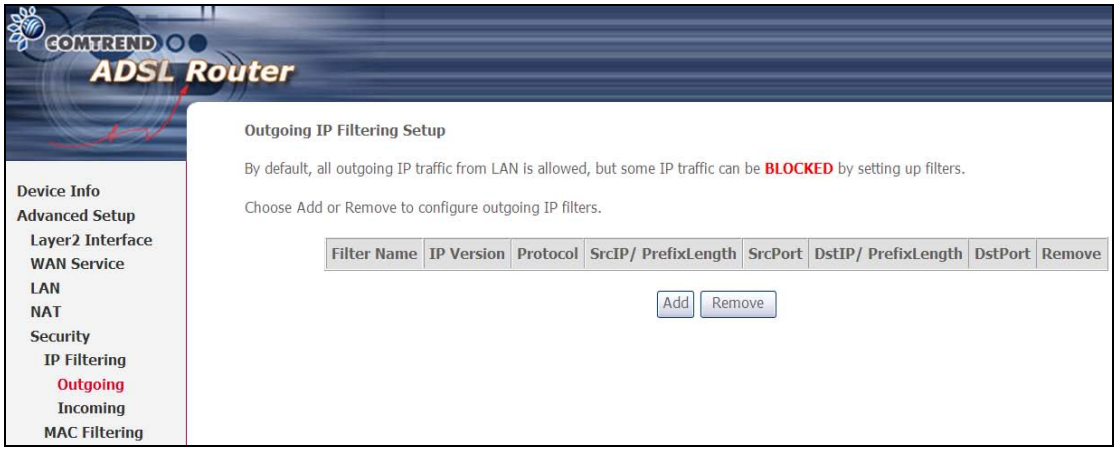
5.5.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

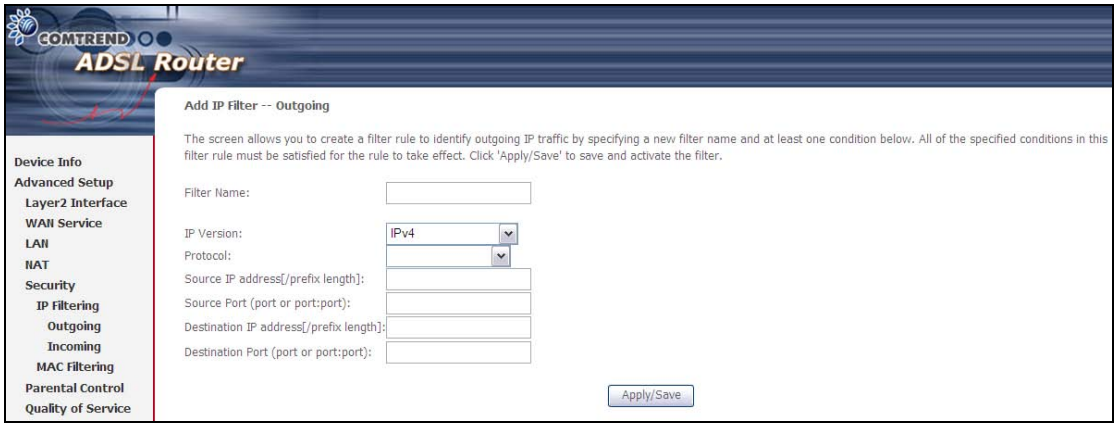
NOTE:	This function is not available when in bridge mode. Instead, 5.5.2 MAC Filtering (pg. 41) performs a similar function.

OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.



To add a filter (to block some outgoing IP traffic), click the **Add** button.
On the following screen, enter your filter criteria and then click **Apply/Save**.

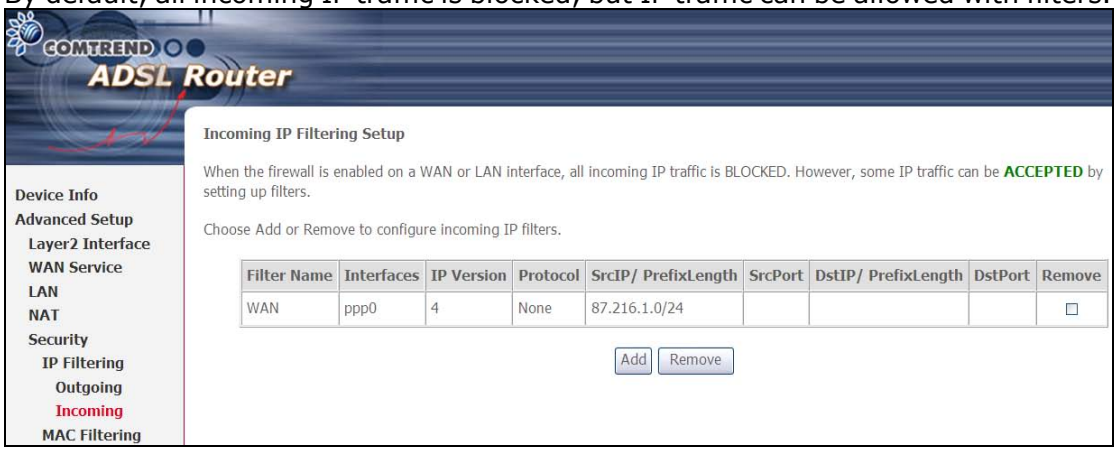


Consult the table below for field descriptions.

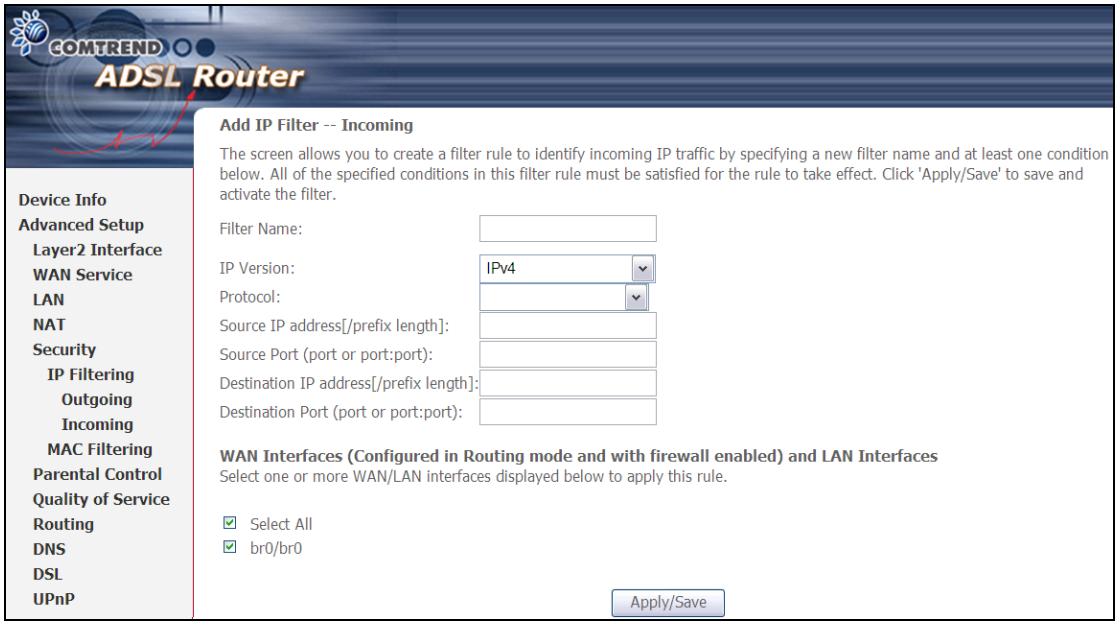
Field	Description
Filter Name	The filter rule label.
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.



To add a filter (to allow incoming IP traffic), click the **Add** button.
On the following screen, enter your filter criteria and then click **Apply/Save**.



Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

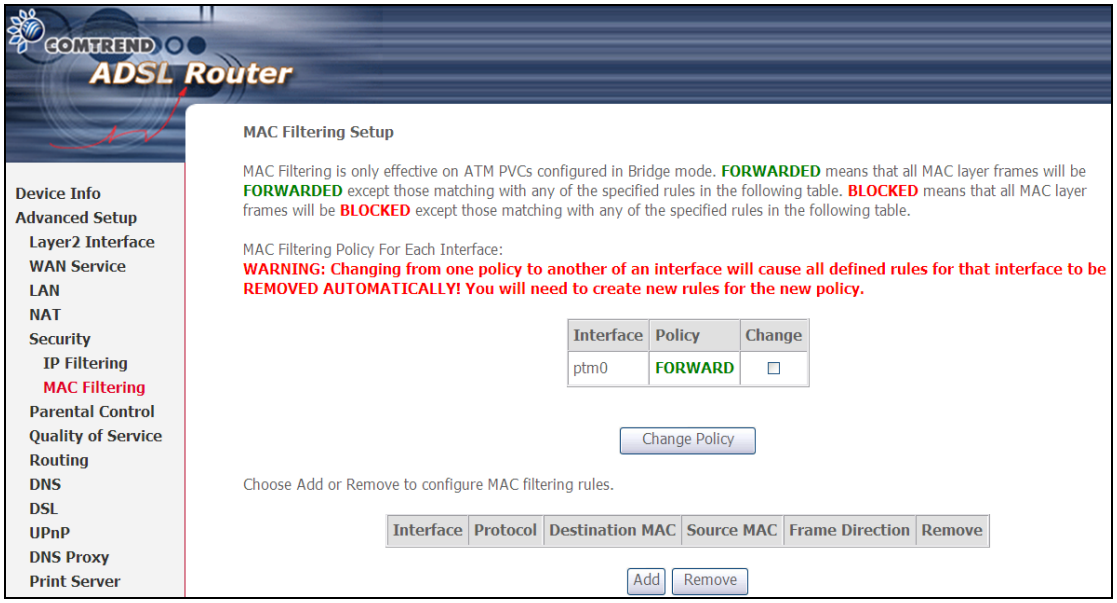
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

5.5.2 MAC Filtering

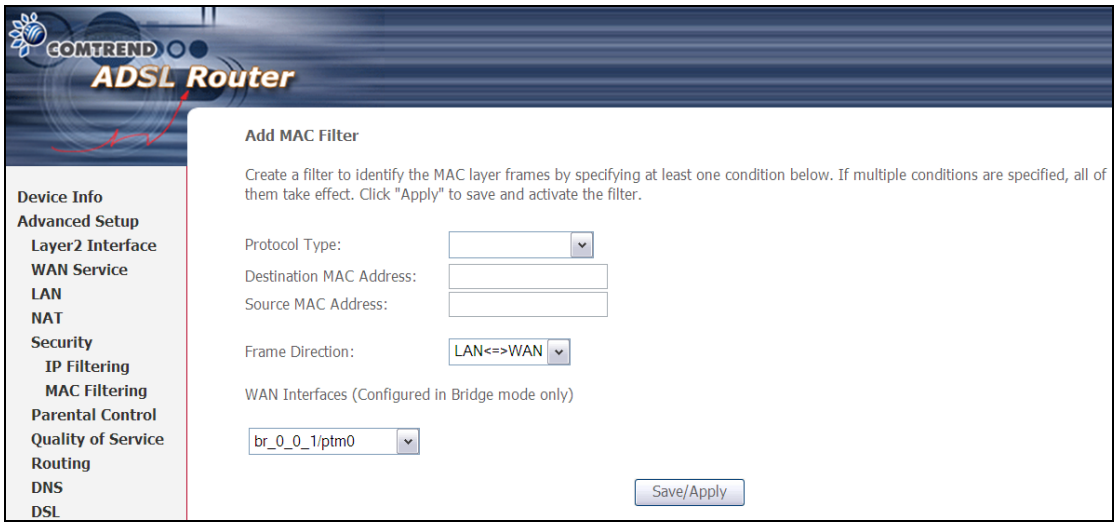
NOTE: This option is only available in bridge mode. Other modes use 5.5.1 IP Filtering (pg.39) to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the AR-5382u can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save / Apply** to save and activate the filter rule.



Consult the table below for detailed field descriptions.

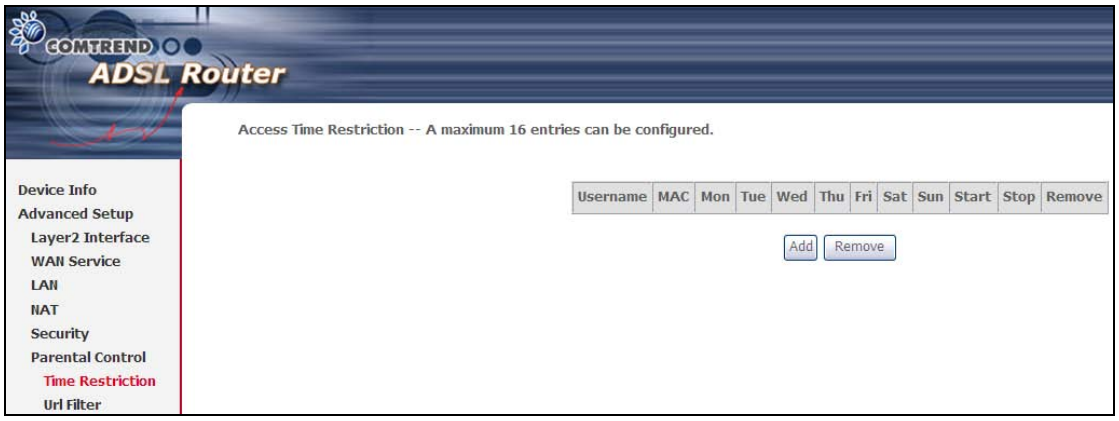
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface.

5.6 Parental Control

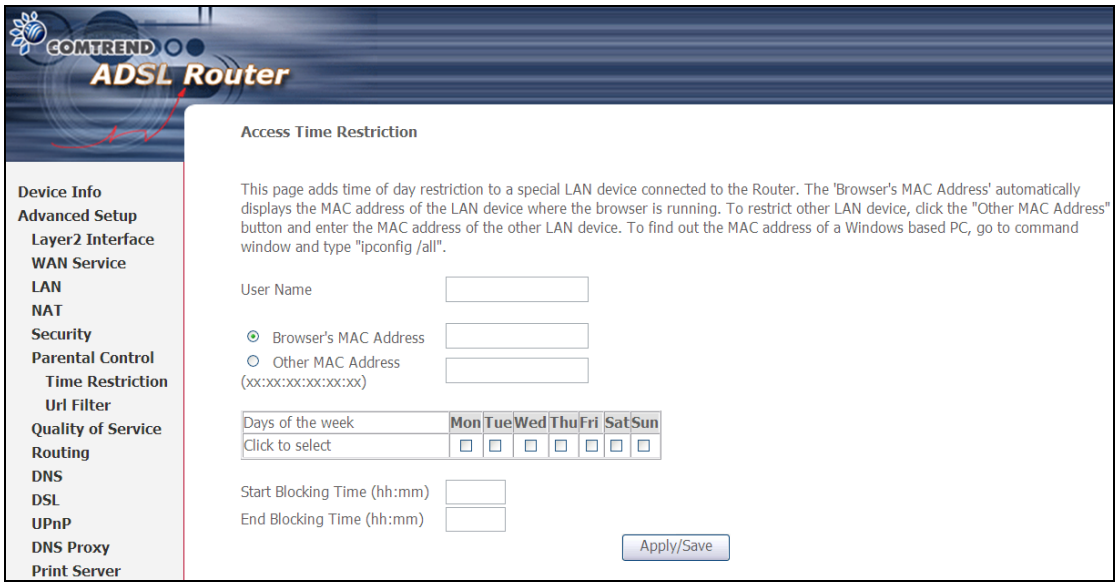
This selection provides WAN access control functionality.

5.6.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in 8.4 Internet Time, so that the scheduled times match your local time.



Click **Add** to display the following screen.

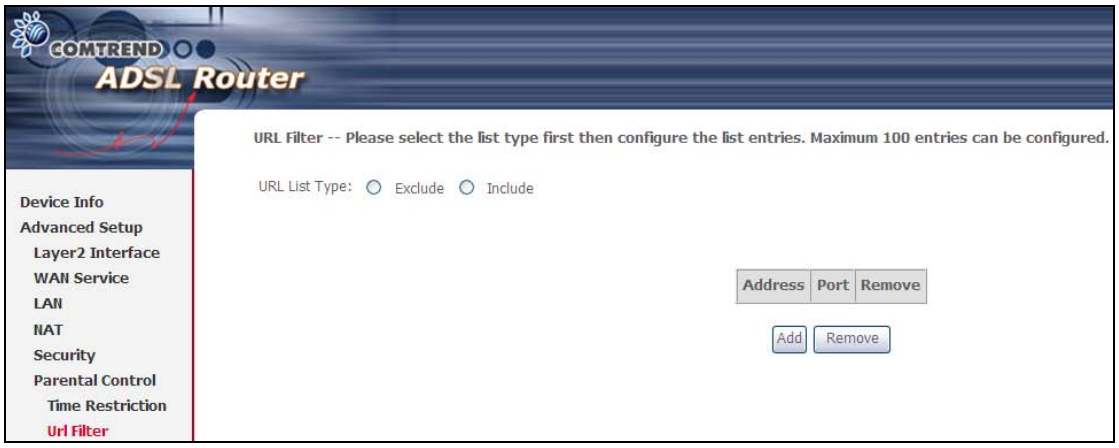


See below for field descriptions. Click **Apply / Save** to add a time restriction.

User Name: A user-defined label for this restriction.
Browser's MAC Address: MAC address of the PC running the browser.
Other MAC Address: MAC address of another LAN device.
Days of the Week: The days the restrictions apply.
Start Blocking Time: The time the restrictions start.
End Blocking Time: The time the restrictions end.

5.6.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.



Click **Add** to display the following screen.

Enter the URL address and port number then click **Save / Apply** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.

A maximum of 100 entries can be added to the URL Filter list.
Tick the **Exclude** radio button to deny access to the websites listed.
Tick the **Include** radio button to restrict access to only those listed websites.

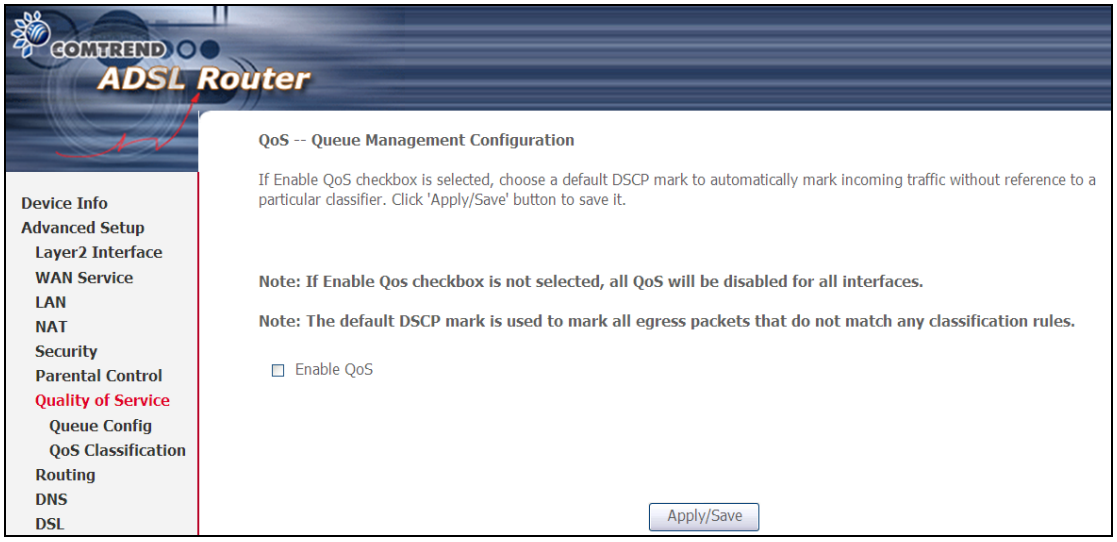
5.7 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.
(see Appendix F - Connection Setup for detailed PVC setup instructions).

5.7.1 Queue Management Configuration

To Enable QoS tick the checkbox ☑ and select a Default DSCP Mark.

Click **Apply / Save** to activate QoS.



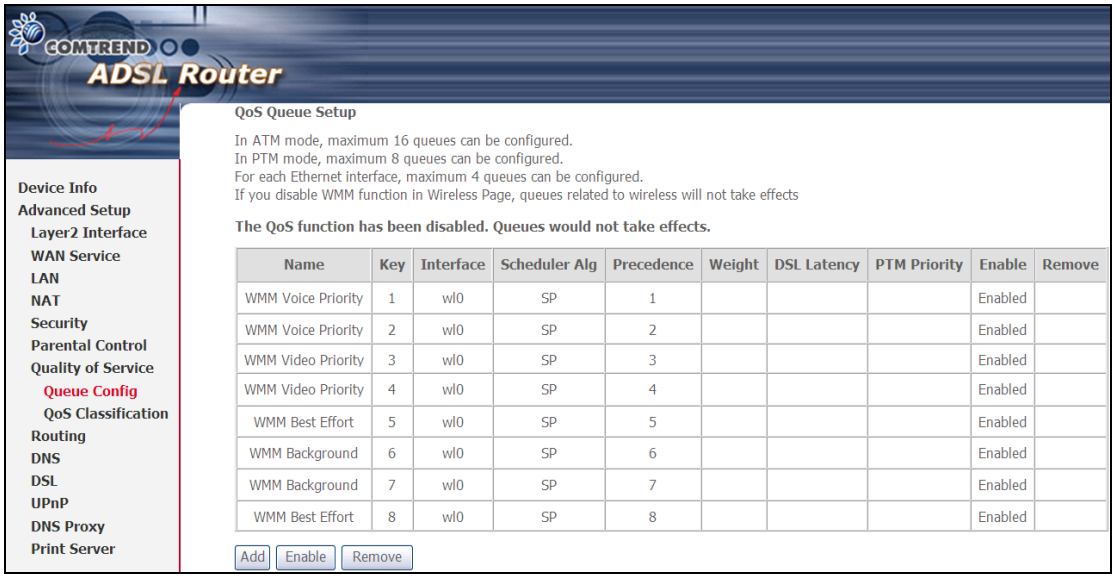
QoS and **DSCP Mark** are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

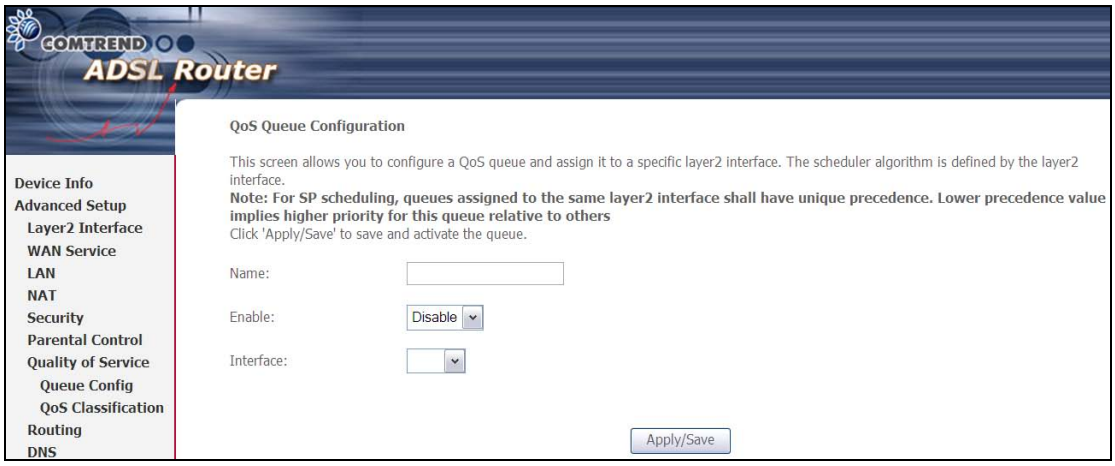
Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

5.7.2 Queue Configuration

This function follows the Differentiated Services rule of IP QoS. You can create a new Queue entry by clicking the **Add** button. Enable and assign an interface and precedence on the next screen. Click **Save/Reboot** on this screen to activate it.



Click **Enable** to activate the QoS Queue. Click **Add** to display the following screen.



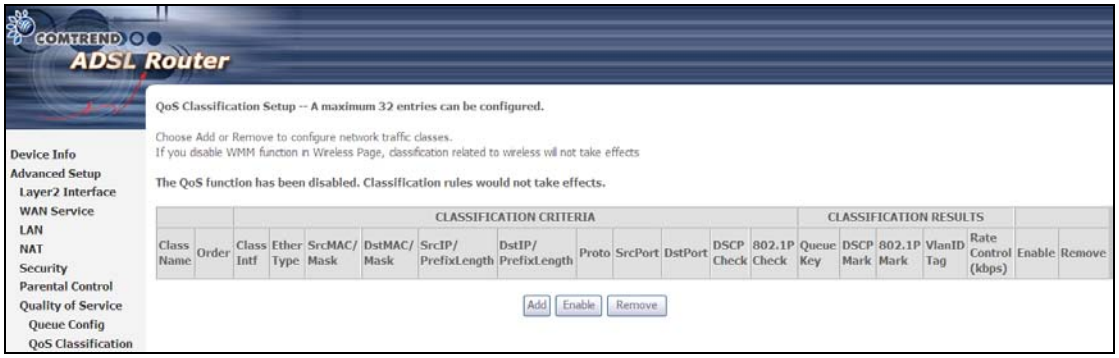
Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

Interface: Assign the entry to a specific network interface (QoS enabled).

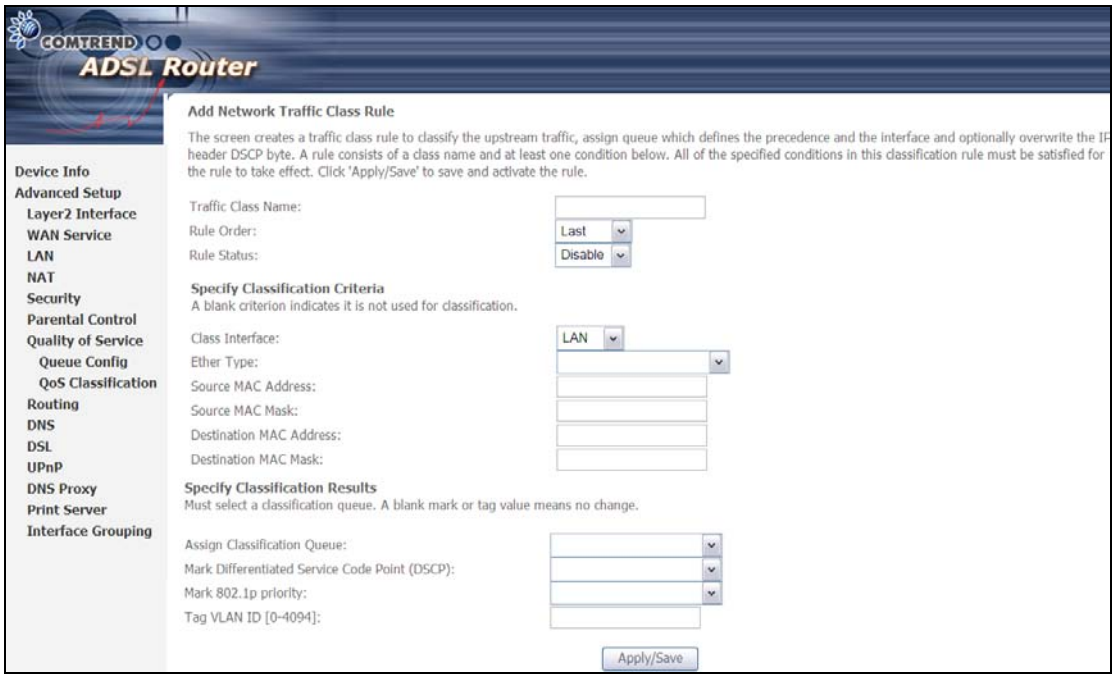
5.7.3 QoS Classification

The network traffic classes are listed in the following table.



Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one logical condition. All the conditions specified in the rule must be satisfied for it to take effect.



Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Class Interface	Select an interface (i.e. Local, eth0-4, wl0)

Field	Description
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in Destination MAC Address.
Classification Results	
Assign Classification Queue	The queue configurations are presented in this format: "Interfacename&Prece P&Queue Q" where P and Q are the Precedence and Queue Key values for the corresponding Interface as listed on the Queue Config screen.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. Lower values have higher priority.
Tag VLAN ID	Enter a 802.1Q VLAN ID tag [2-4094]

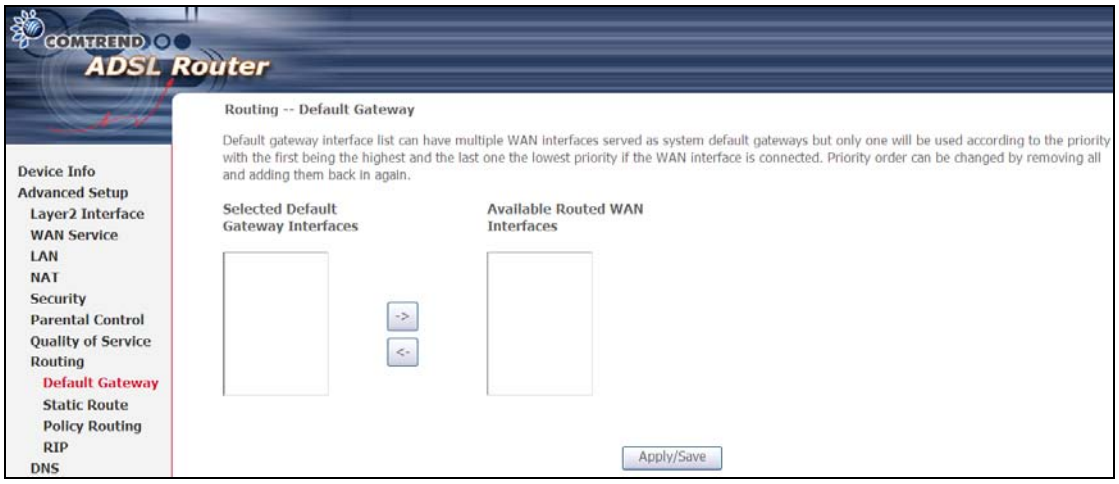
5.8 Routing

This following routing functions are accessed from this menu:
Default Gateway, Static Route, Policy Routing, RIP and **IPv6 Static Route**.

NOTE:	In bridge mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.

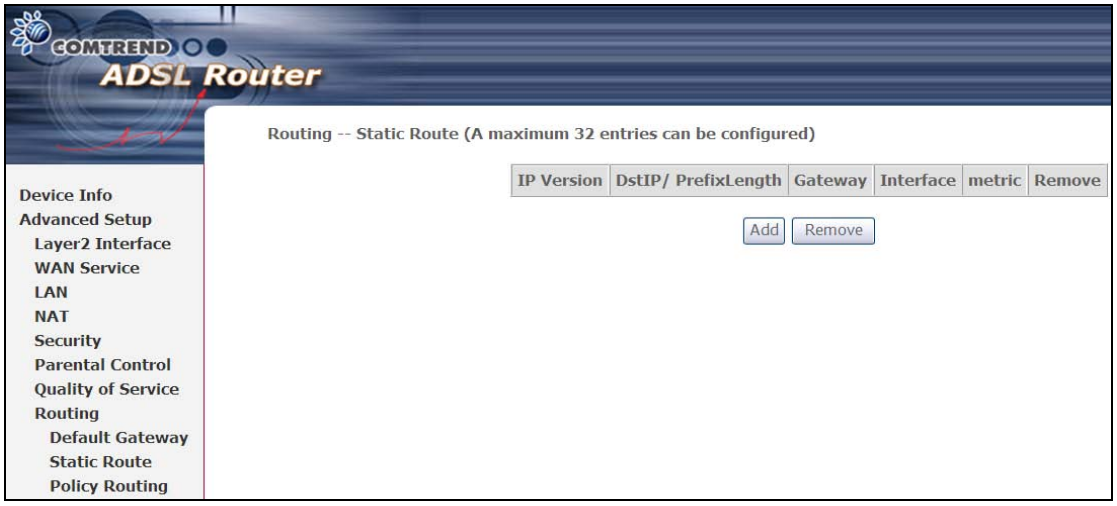
5.8.1 Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

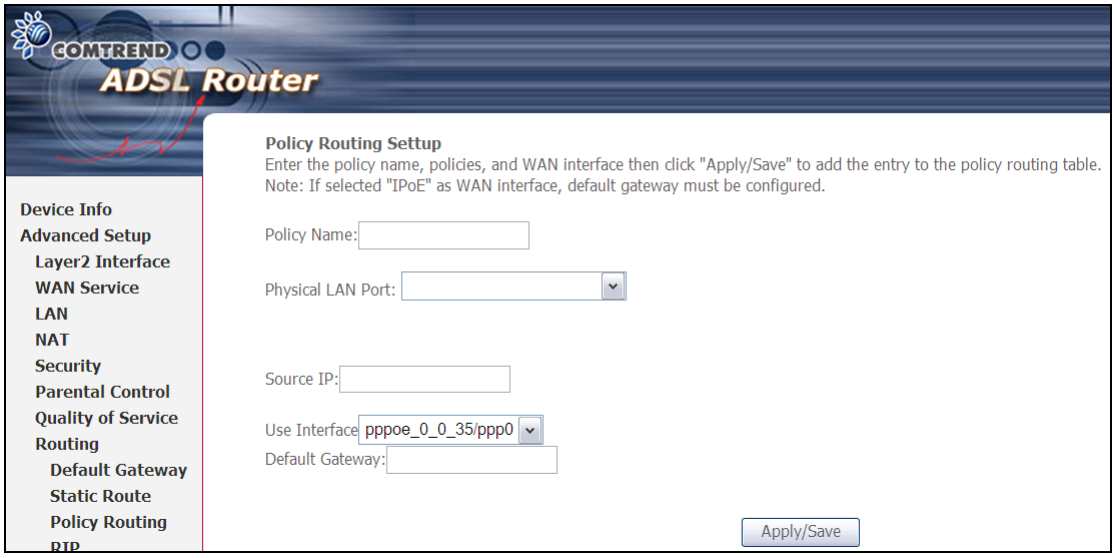


5.8.2 Static Route

This option allows for the configuration of static routes by destination IP.
Click **Add** to create a static route or click **Remove** to delete a static route.



After clicking **Add** the following screen will display.



Input the Destination IP Address, select the interface type, Input the Gateway IP, (and the Metric number if required). Then, click **Apply / Save** to add an entry to the routing table.

5.8.3 RIP

To activate RIP, select the **Enabled** radio button for Global RIP Mode. To configure an individual interface (PVC), select the desired RIP Version and Operation, and then select the **Enabled** checkbox ☑ for that interface (PVC). Click **Save / Apply** to save the configuration and start/stop RIP (based on the Global RIP mode selected).

5.9 DNS

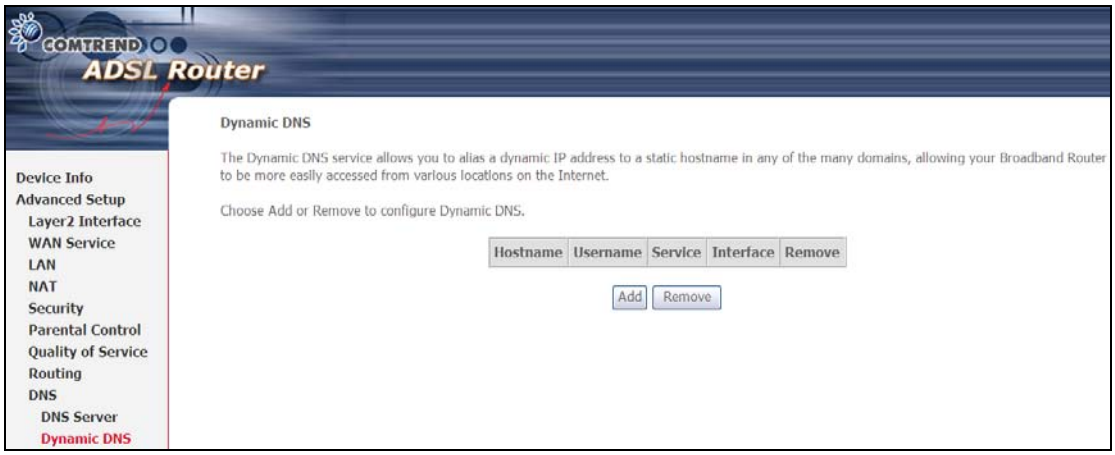
5.9.1 DNS Server

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

Click Apply/Save to save the new configuration.

5.9.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the AR-5382u to be more easily accessed from various locations on the Internet.



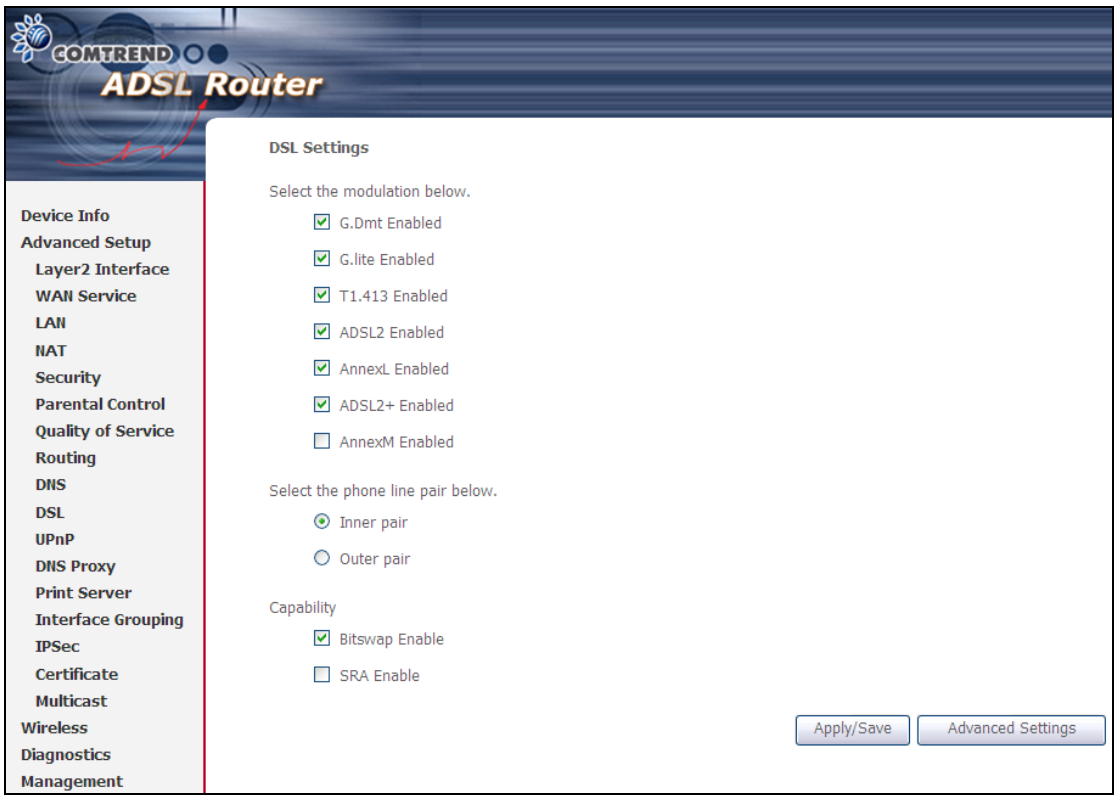
To add a dynamic DNS service, click **Add**. The following screen will display.

Consult the table below for field descriptions.

Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

5.10 DSL

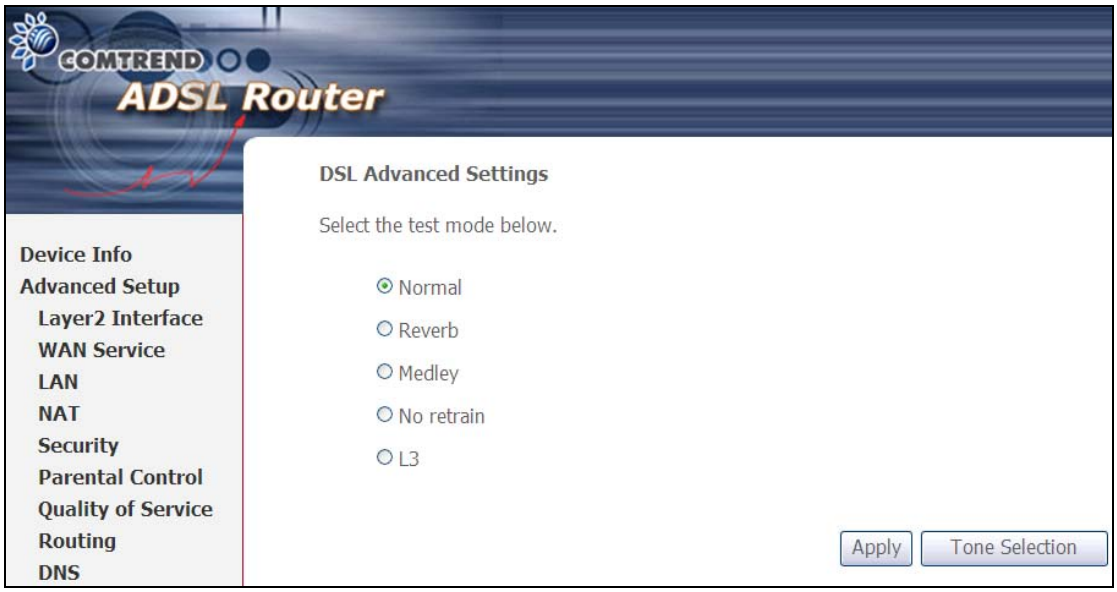
The DSL Settings screen allows for the selection of DSL modulation modes.
For optimum performance, the modes selected should match those of your ISP.



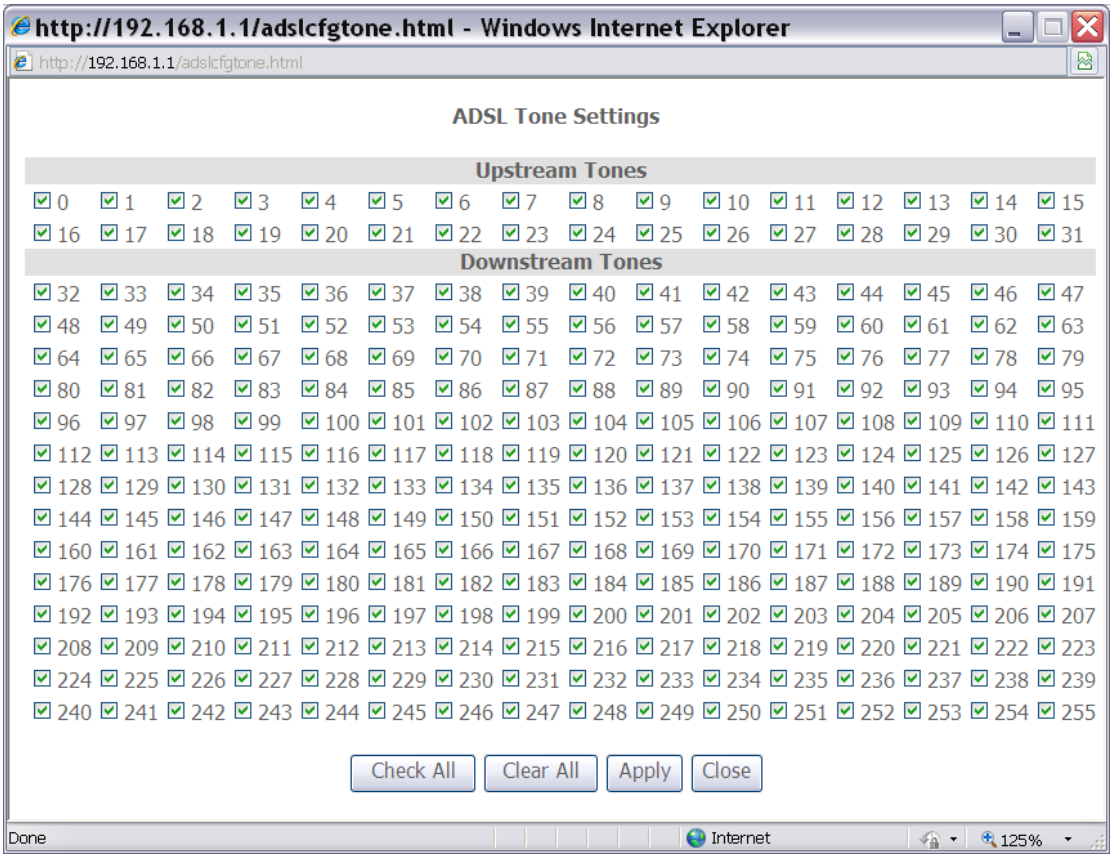
DSL Mode	Data Transmission Rate - Mbps (Megabits per second)	
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates	
ADSL2+	Downstream: 24 Mbps	Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps	Upstream: 3.5 Mbps
Options	**Description**	
Inner/Outer Pair	Select the inner or outer pins of the twisted pair (RJ11 cable)	
Bitswap Enable	Enables adaptive handshaking functionality	
SRA Enable	Enables Seamless Rate Adaptation (SRA)	

Advanced DSL Settings

Click **Advanced Settings** to reveal additional options. On the following screen you can select a test mode or modify tones by clicking **Tone Selection**. Click **Apply** to implement these settings and return to the previous screen.

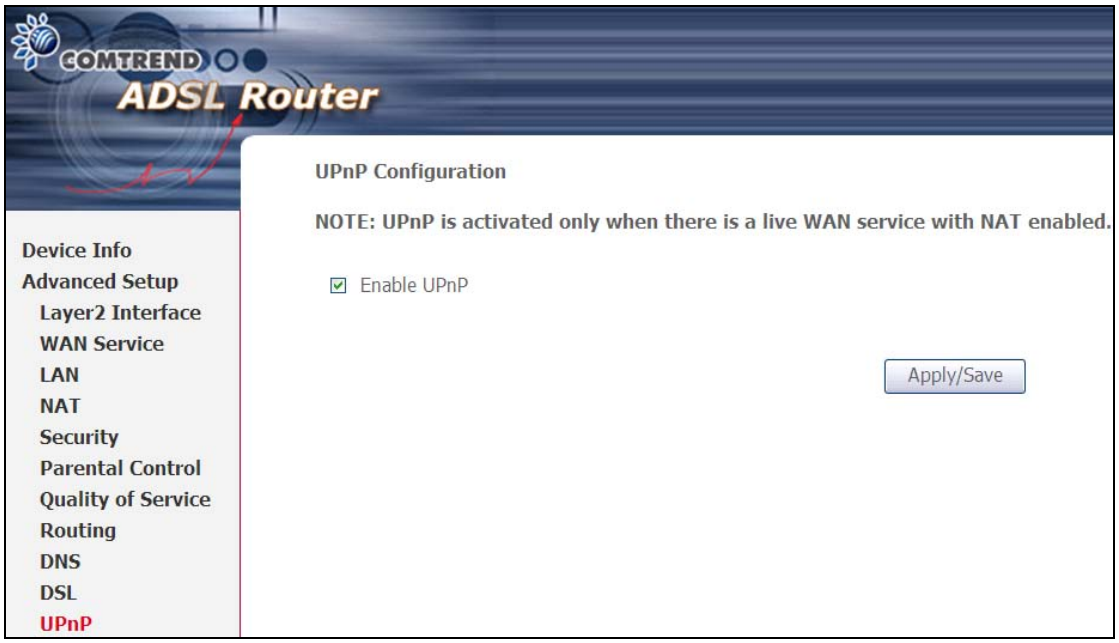


On this screen you select the tones you want activated, then click **Apply** and **Close**.

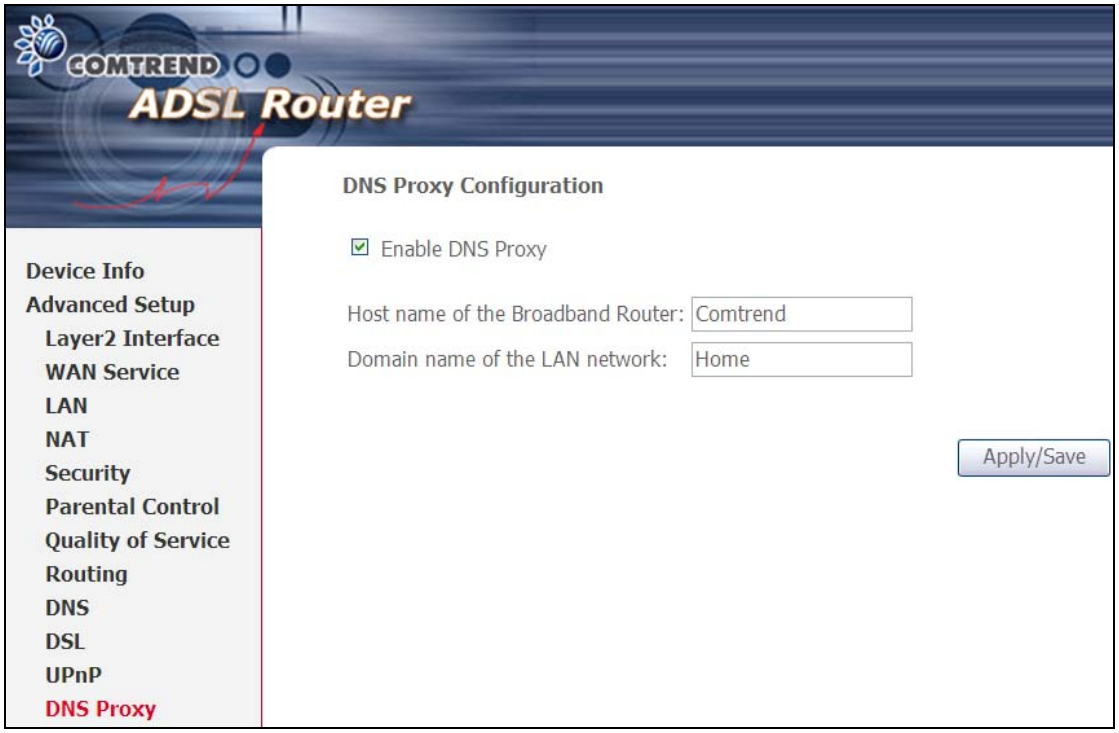


5.11 UPnP

Select the checkbox ☑ provided and click **Apply / Save** to enable UPnP protocol.

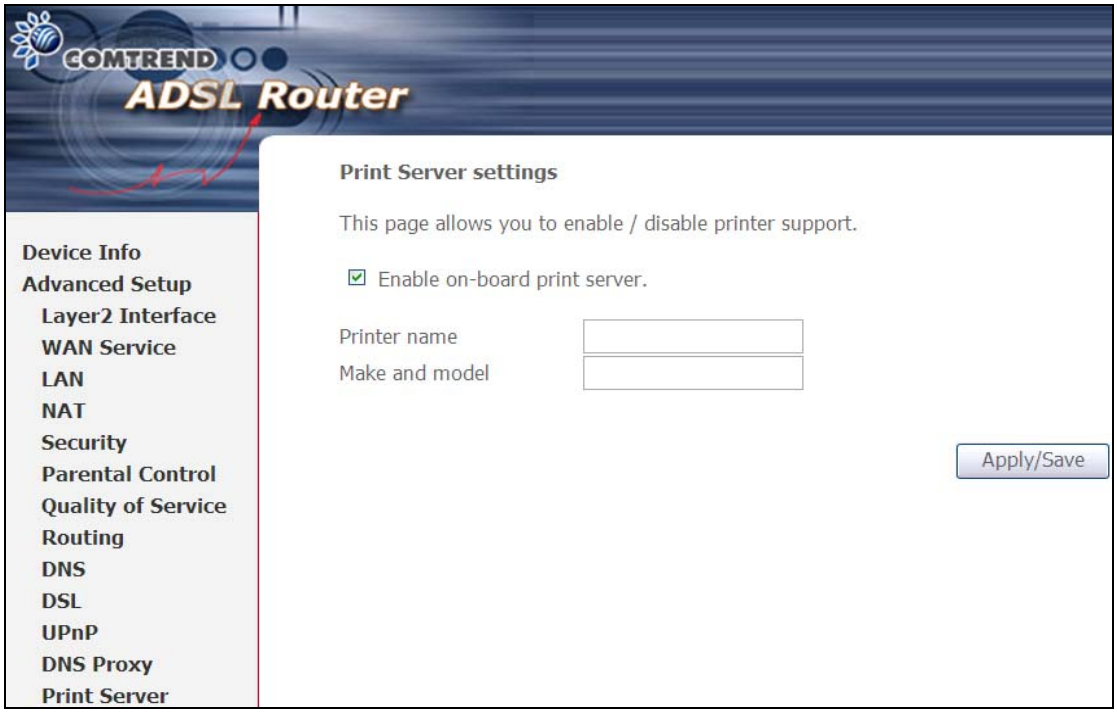


5.12 DNS Proxy



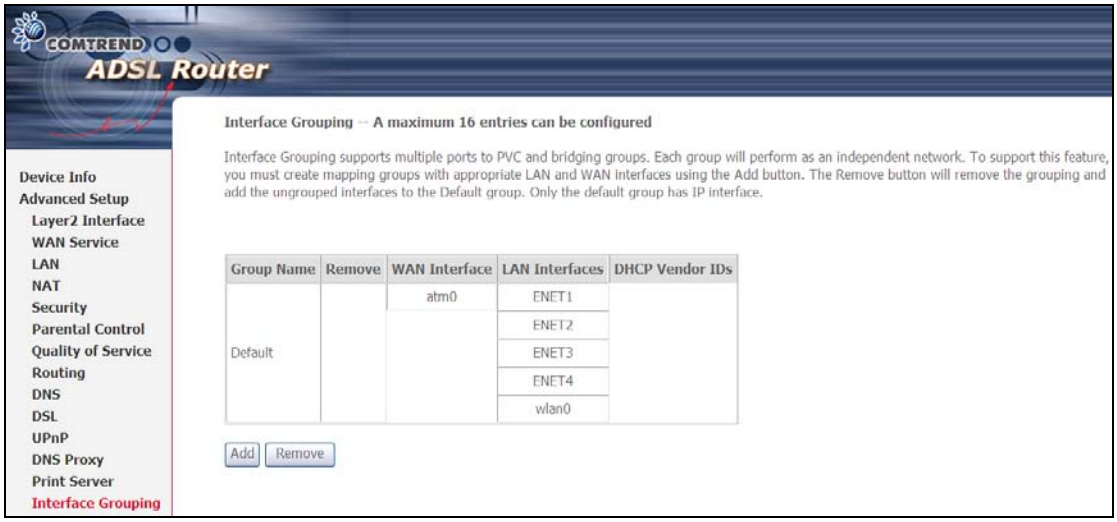
5.13 Print Server

The AR-5382u can provide printer support through an optional USB2.0 host port. If your device has this port, refer to Appendix E - Printer Server for detailed setup instructions.



5.14 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.
The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.



To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown onscreen.

Automatically Add Clients With Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ENET1, ENET2, ENET3, and ENET4.

The Interface Grouping configuration will be:

1. Default: ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

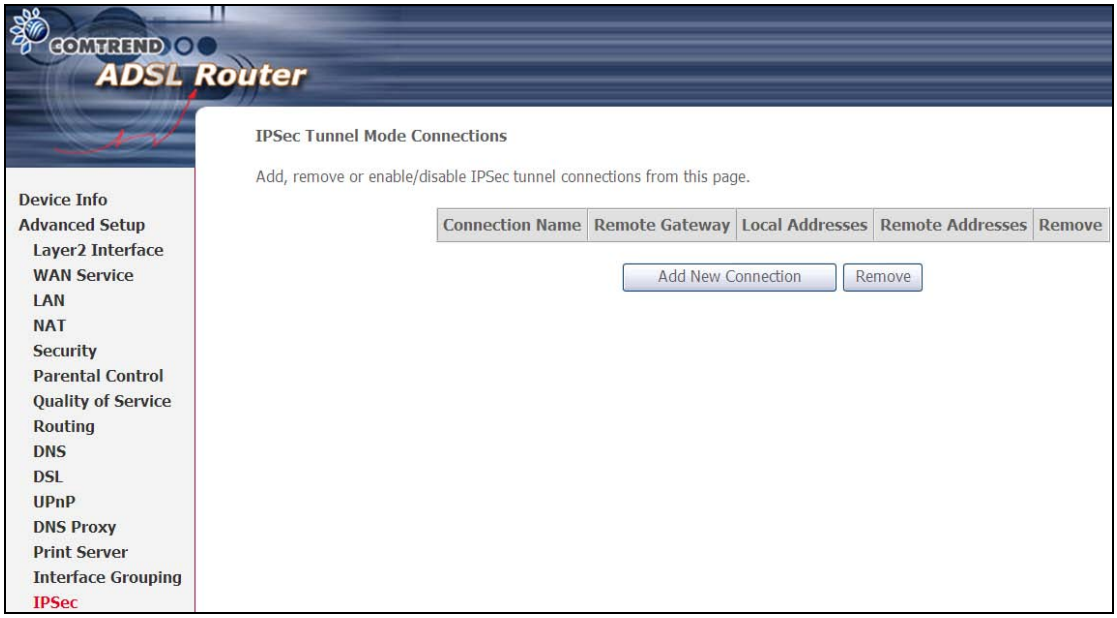
If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

If a set-top box is connected to ENET1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ENET2, ENET3, and ENET4
2. Video: nas_0_36, nas_0_37, nas_0_38, and ENET1.

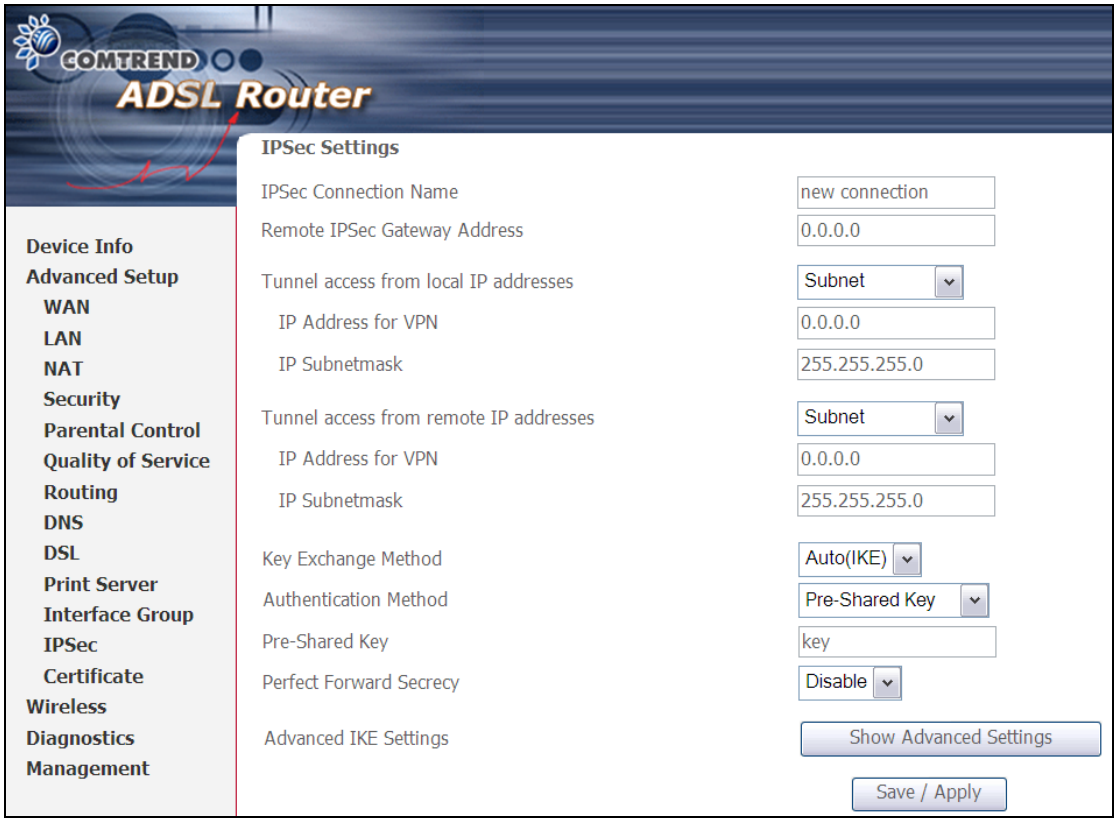
5.15 IPSec

You can add, edit or remove IPSec tunnel mode connections from this page.



Click **Add New Connection** to add a new IPSec termination rule.

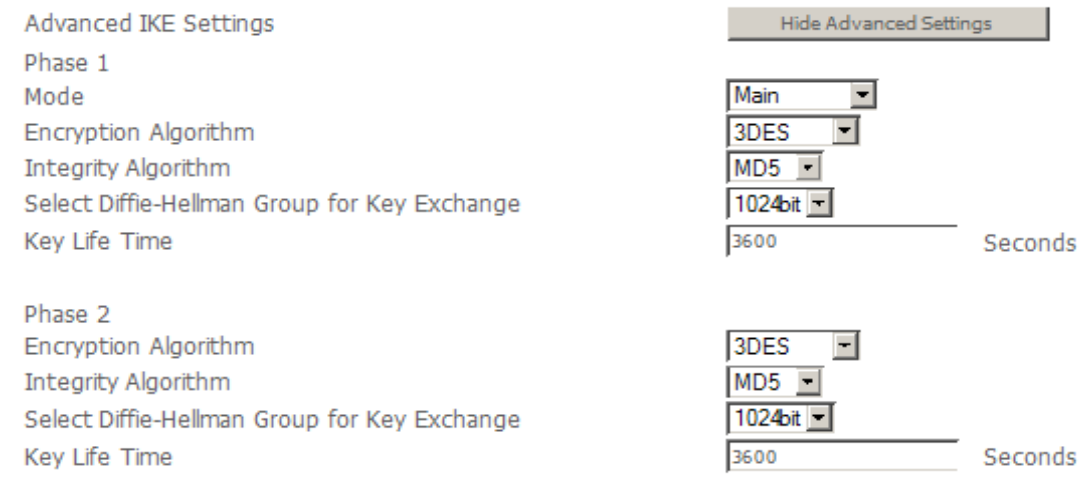
The following screen will display.



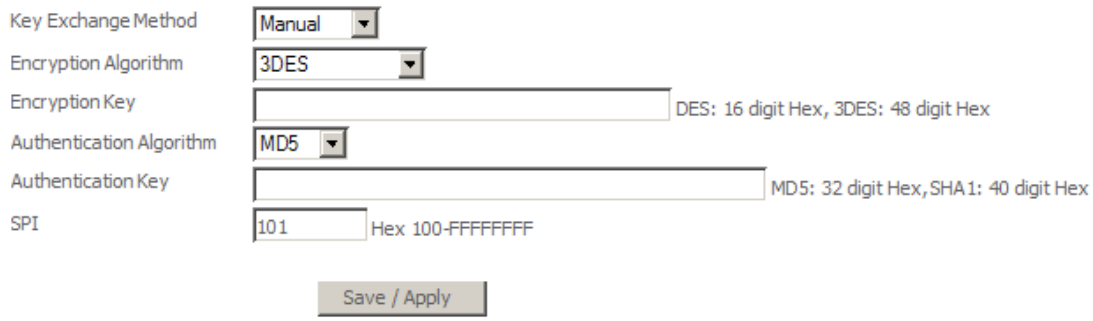
IPSec Connection Name	User-defined label
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. F or Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.
	
Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

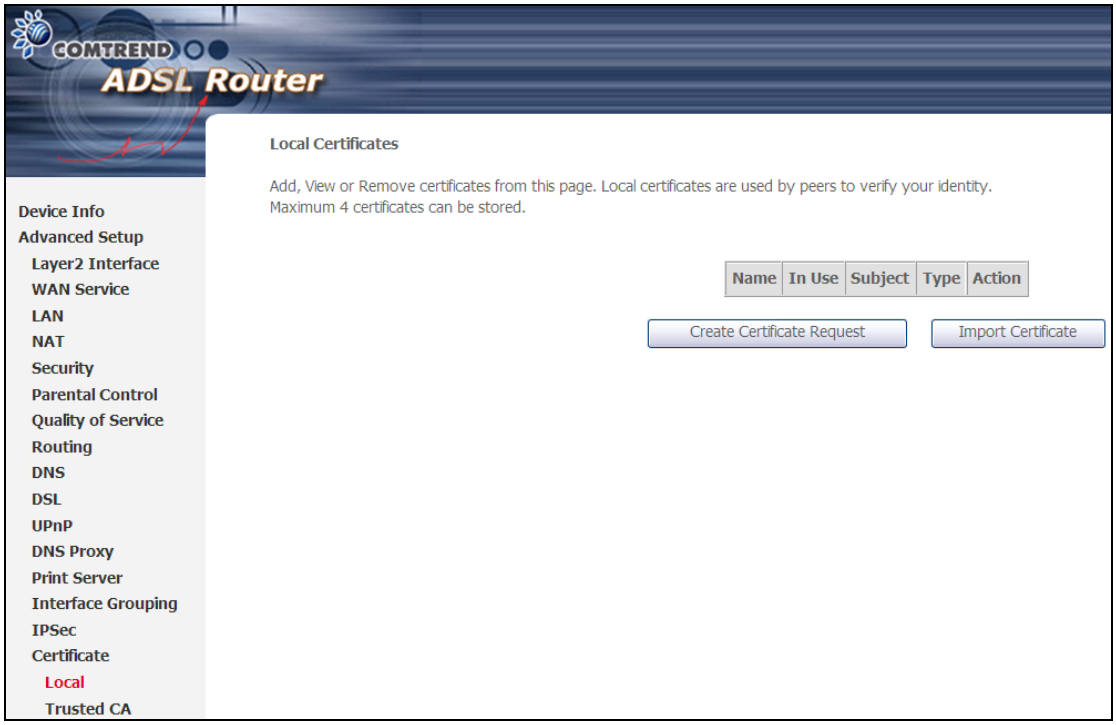
The Manual key exchange method options are summarized in the table below.

Manual Key Exchange Method	
	
Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

5.16 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

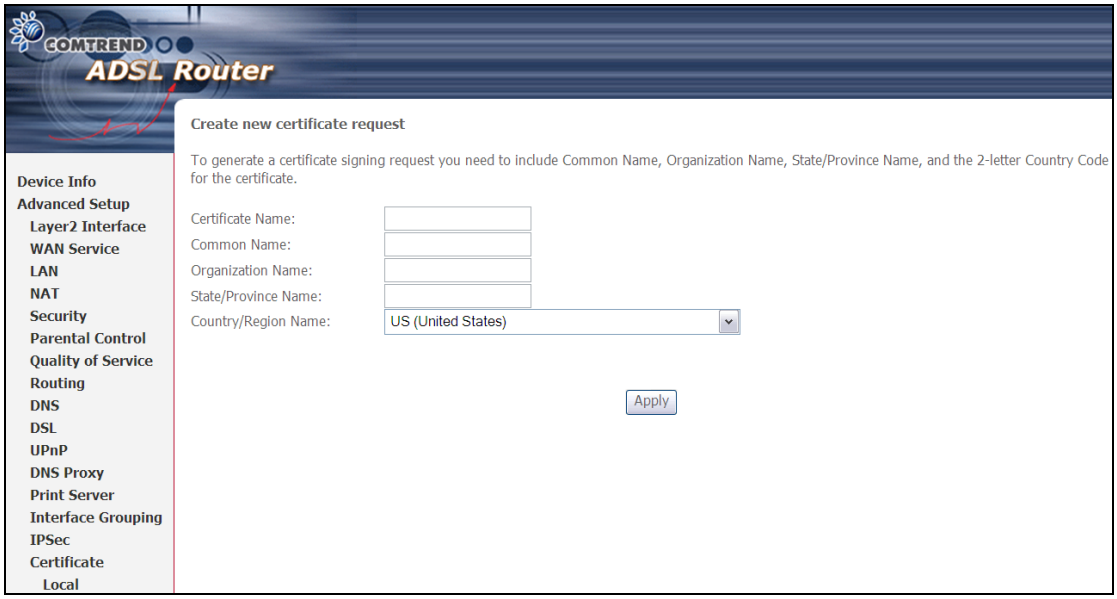
5.16.1 Local



CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.



The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

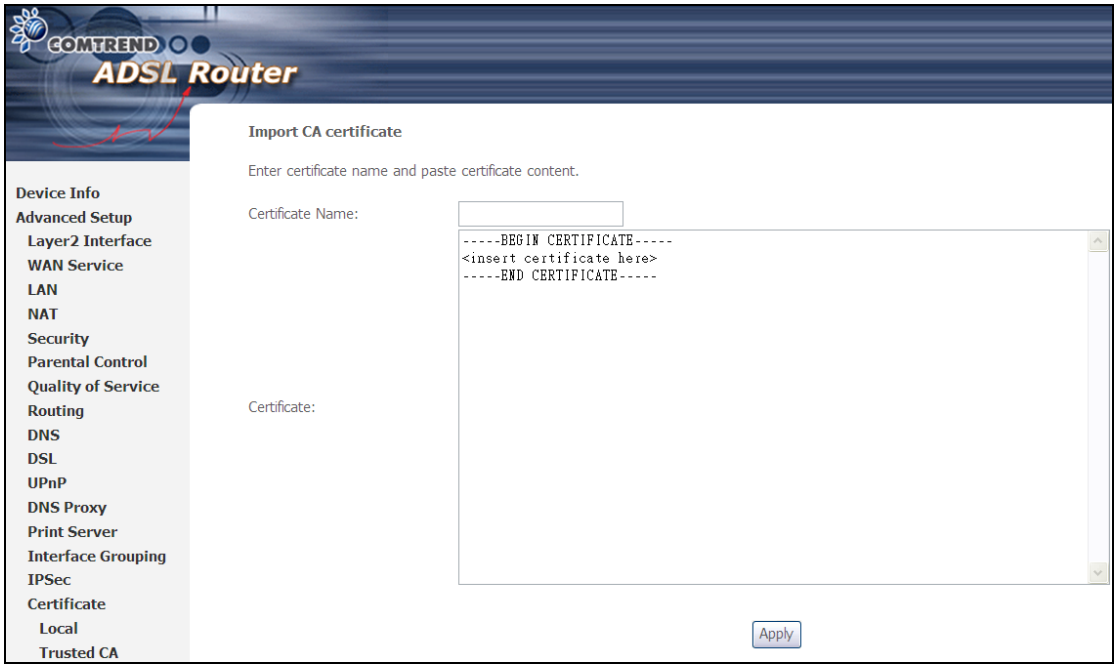
Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.

Enter a certificate name and click **Apply** to import the local certificate.

5.16.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.

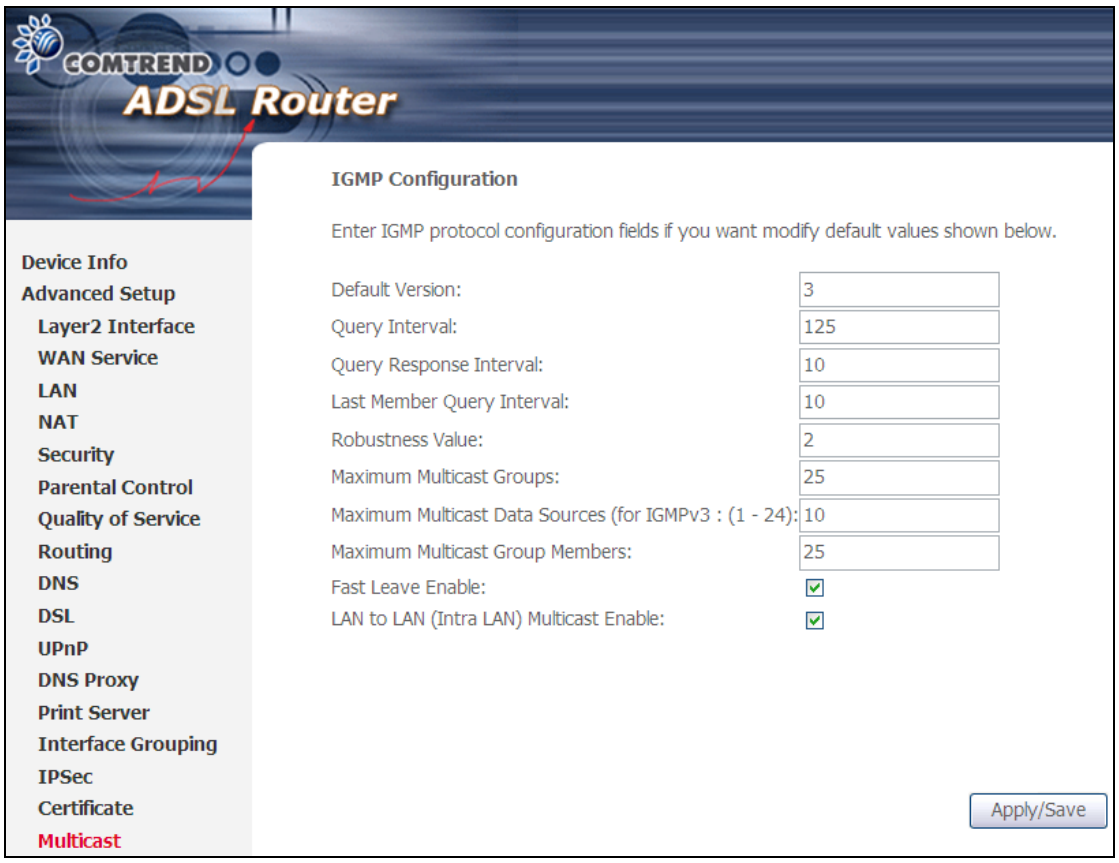
Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Enter a certificate name and click **Apply** to import the CA certificate.

5.17 Multicast

Input new IGMP protocol configuration fields if you want modify default values shown. Then click Apply/Save.

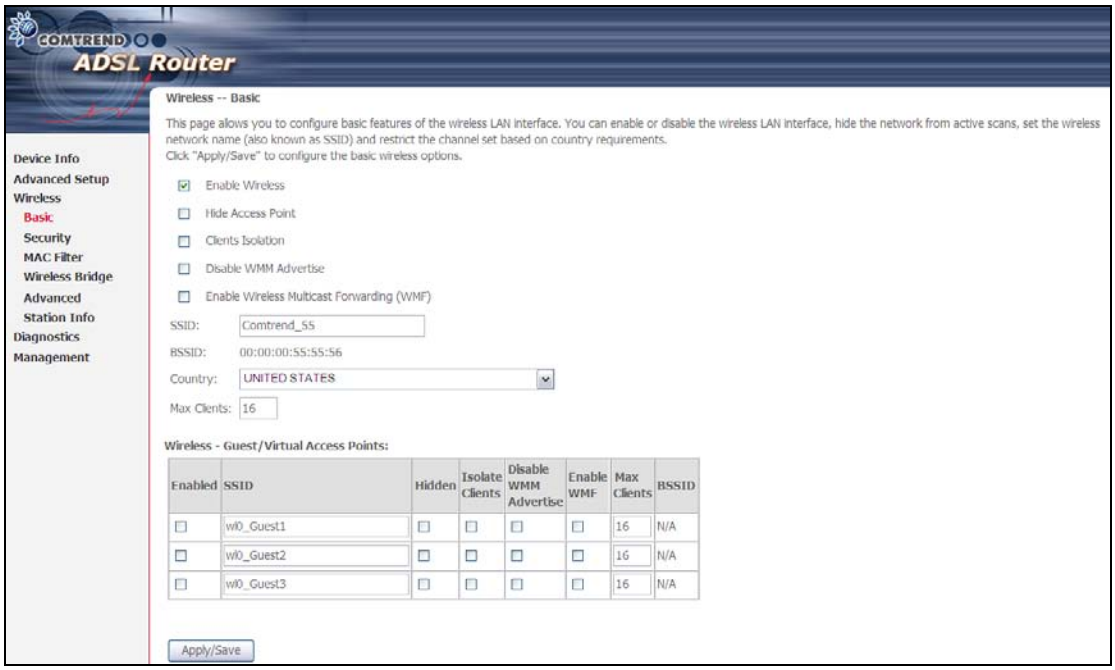


Chapter 6 Wireless

The Wireless menu provides access to the wireless options discussed below.

6.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



Click **Save / Apply** to apply the selected wireless options.

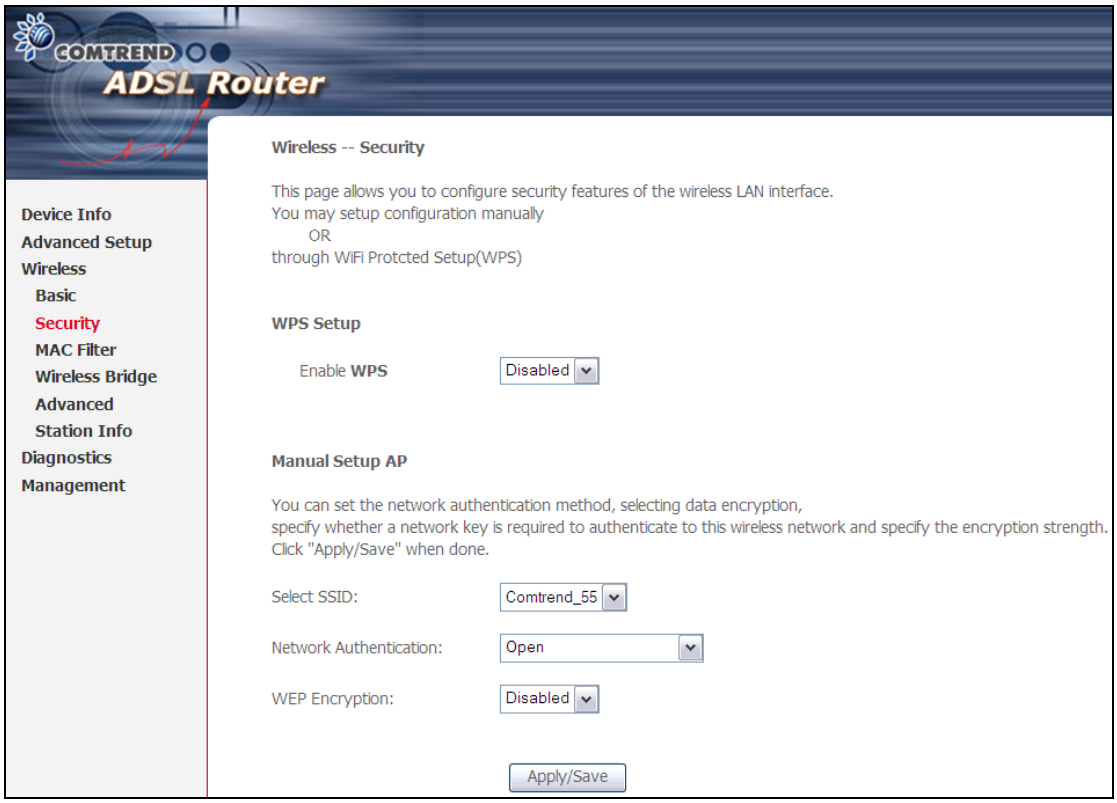
Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.

Option	Description
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable Wireless Multicast Forwarding	Select the checkbox ☑ to enable this function.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Enable WMF**, **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

6.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



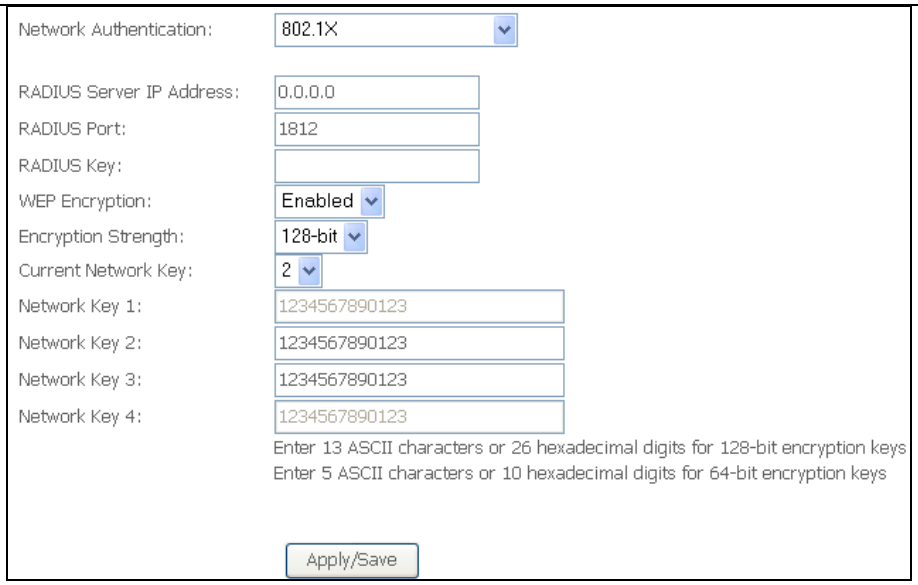
Click **Save / Apply** to implement new configuration settings.

WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically (see 6.2.1 WPS) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

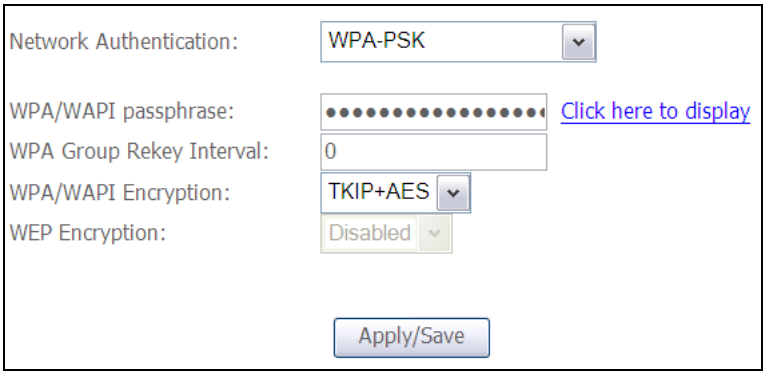
Select SSID
Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



The settings for WPA authentication are shown below.

The settings for WPA-PSK authentication are shown next.



WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The AR-5382u has both a WPS button on the device and a virtual button accessible from the web user interface (WUI).

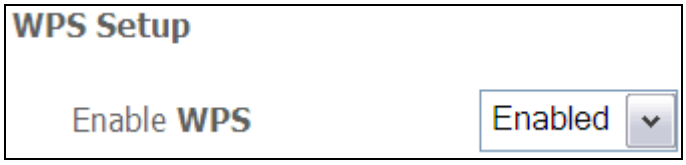
Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".

NOTE: WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

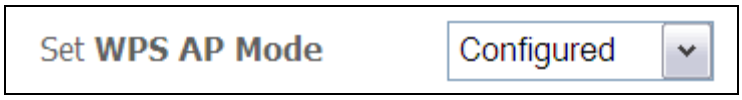
To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

I. Setup

Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.



Step 2: Set the WPS AP Mode. **Configured** is used when the AR-5382u will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the AR-5382u.

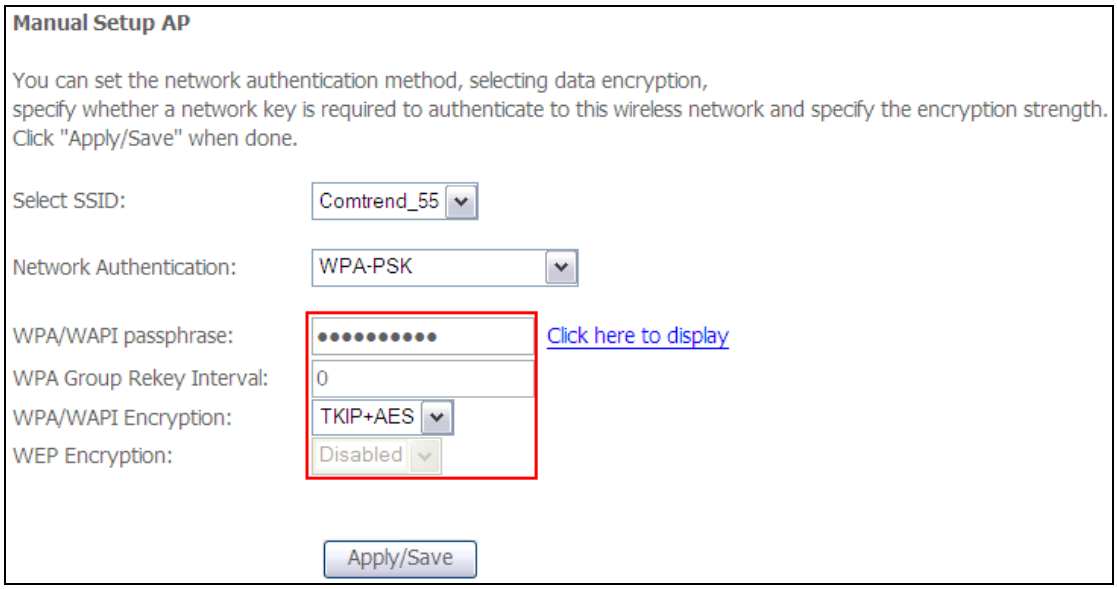


NOTES: Your client may or may not have the ability to provide security settings to the AR-5382u. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities.

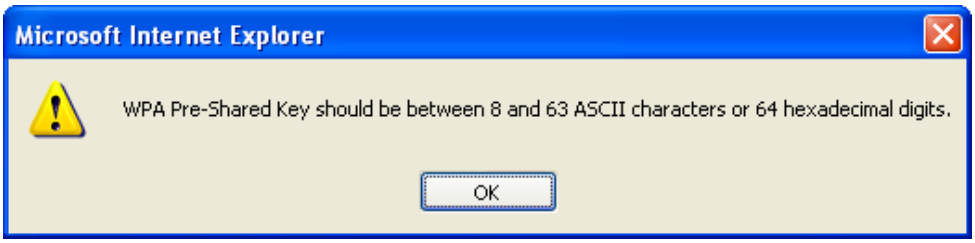
In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button (Appendix D - WPS External Registrar has detailed instructions).

II. NETWORK AUTHENTICATION

Step 3: Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.



Step 4: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You will see the following dialog box if the Key is too short or too long.



Step 5: Click the **Save / Apply** button at the bottom of the screen.

III a. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

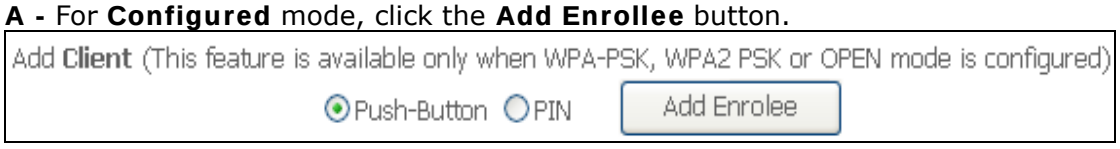
The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

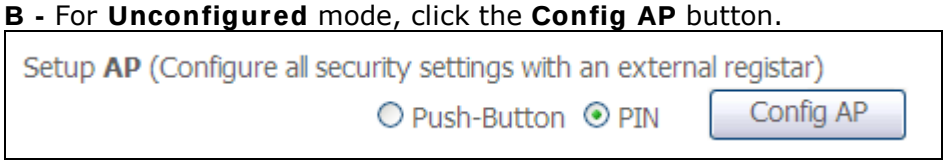
Step 6: **First method: WPS button**
Press the WPS button on the rear panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Second method: WUI virtual button
Select the Push-Button radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

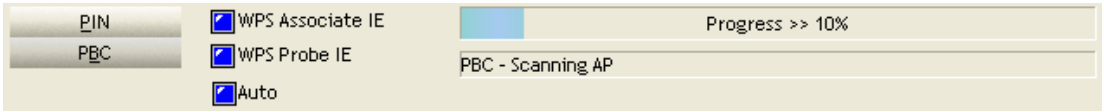
A - For **Configured** mode, click the **Add Enrollee** button.



B - For **Unconfigured** mode, click the **Config AP** button.



Step 7: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

III b. WPS – PIN CONFIGURATION

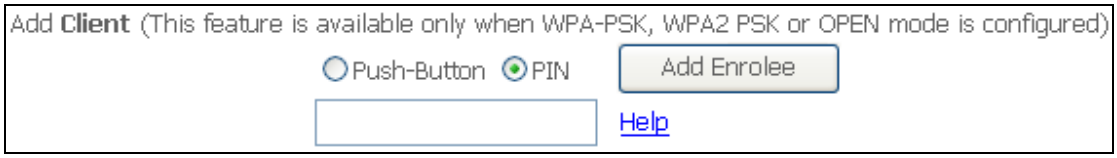
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

Step 6: Select the PIN radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

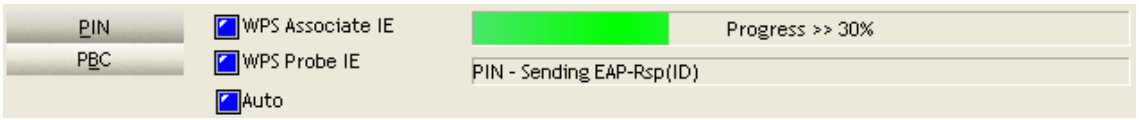
A - For **Configured** mode, enter the client PIN in the box provided and then click the **Add Enrollee** button (see below).



B - For **Unconfigured** mode, click the **Config AP** button.

Step 7: Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

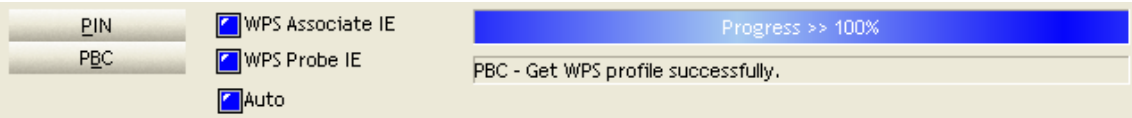
The figure below provides an example of a WPS client PIN function in-progress.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IV. CHECK CONNECTION

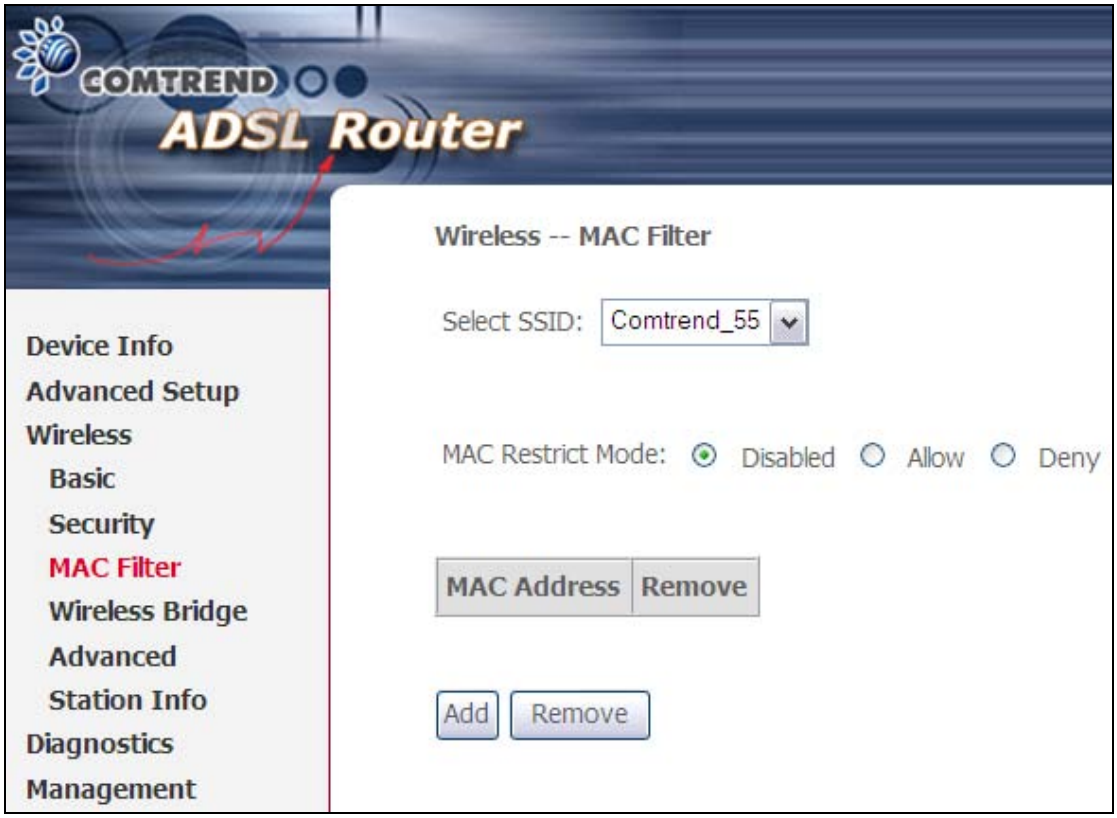
Step 8: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

6.3 MAC Filter

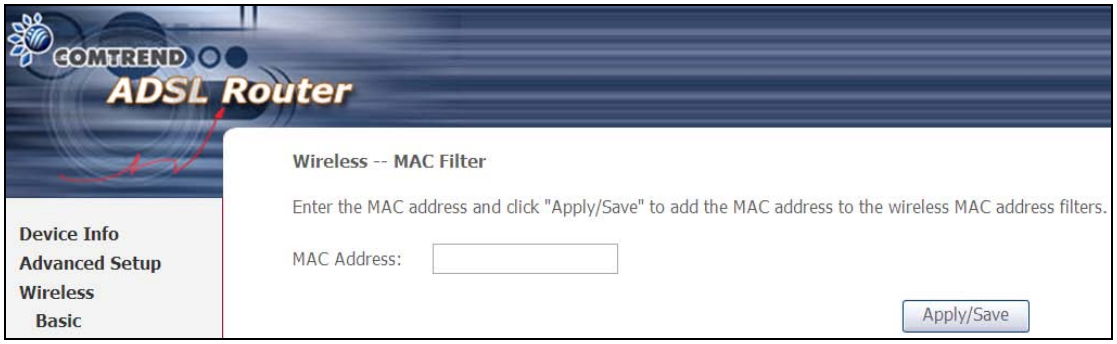
This option allows access to the router to be restricted based upon MAC addresses. To add a MAC Address filter, click the **Add** button shown below. To delete a filter, select it from the MAC Address table below and click the **Remove** button.



Option	Description
Select SSID	Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
MAC Restrict Mode	Disabled: MAC filtering is disabled. Allow: Permits access for the specified MAC addresses. Deny: Rejects access for the specified MAC addresses.
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. A maximum of 60 MAC addresses can be added. Every network device has a unique 48-bit MAC address. This is usually shown as xx.xx.xx.xx.xx.xx, where xx are hexadecimal numbers.

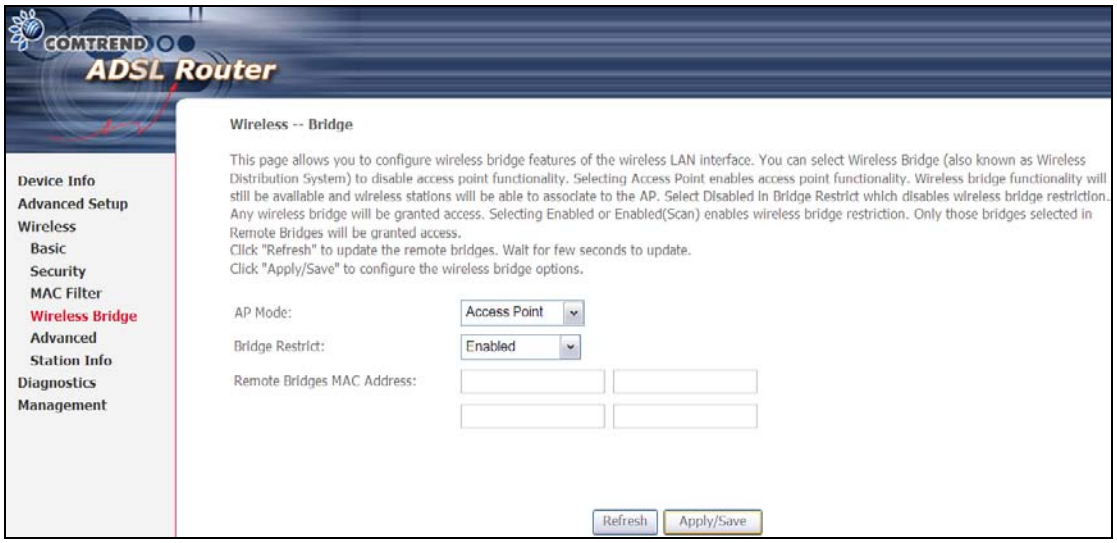
After clicking the **Add** button, the screen below appears.

Enter the MAC address in the box provided and click **Save / Apply**.



6.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WLAN interface. See the table beneath for detailed explanations of the various options.

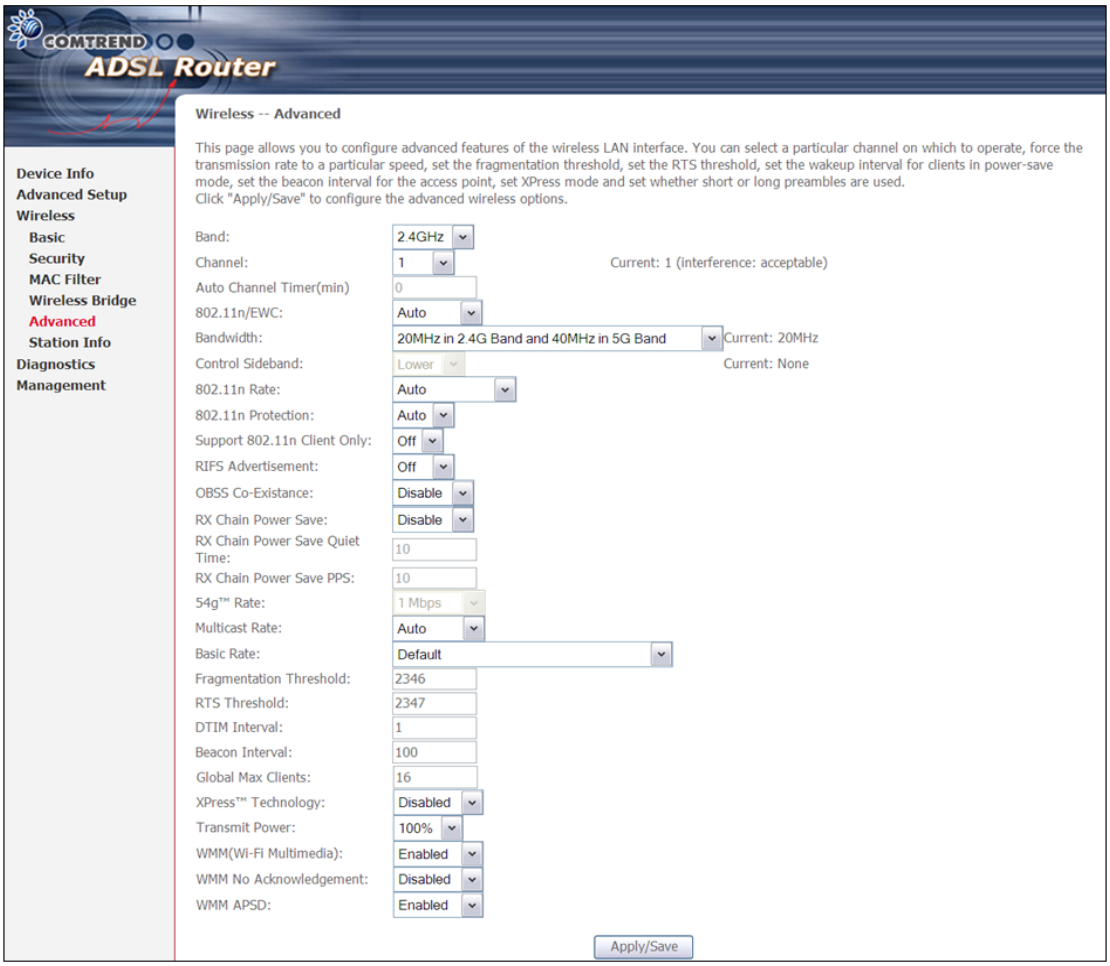


Click **Save / Apply** to implement new configuration settings.

Feature	Description
AP Mode	Selecting **Wireless Bridge** (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting **Access Point** enables AP functionality. In **Access Point** mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting **Disabled** disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click **Refresh** to update the station list when Bridge Restrict is enabled.

6.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Save / Apply** to set new advanced wireless options.



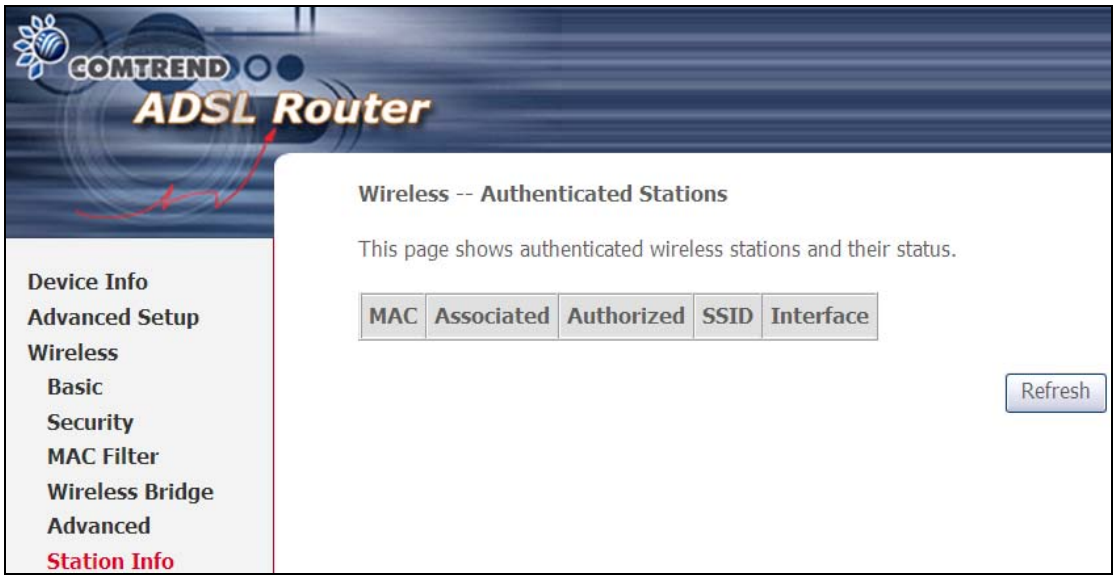
Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)

Field	Description
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g clients access to the router.
RIFS Advertisement	Reduced Interframe Space is the creation of a short time delay between PDUs to improve wireless efficiency.
OBSS Co-Existence	Co-existence between 20 MHZ AND 40 MHZ overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting for basic transmission rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.

Field	Description
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

6.6 Station Info

This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.

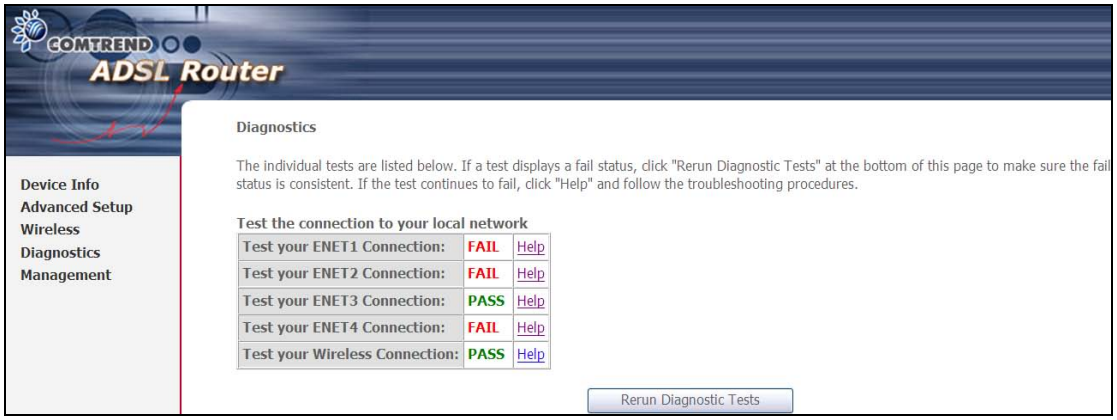


Consult the table below for descriptions of each column heading.

Heading	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

Chapter 7 Diagnostics

The first Diagnostics screen is a dashboard that shows overall connection status.
If a test displays a fail status, click the button to retest and confirm the error.
If a test continues to fail, click Help and follow the troubleshooting procedures.



Chapter 8 Management

Click on the link to jump to a specific section:

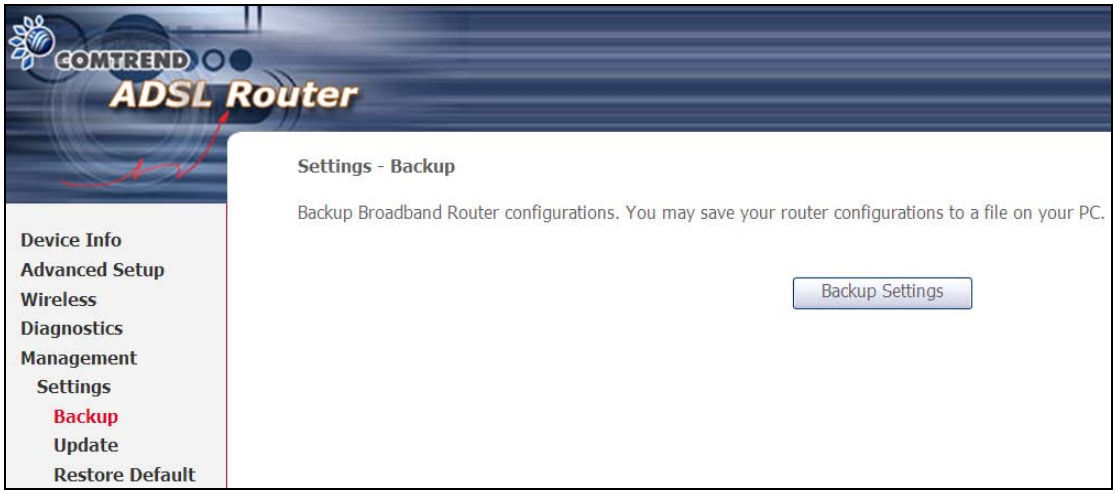
8.1 Settings
8.2 System Log
8.3 TR-069 Client
8.4 Internet Time
8.5 Access Control
8.6 Update Software
8.7 Reboot

8.1 Settings

This includes 8.1.1 Backup Settings, 8.1.2 Update Settings, and 8.1.3 Restore Default screens.

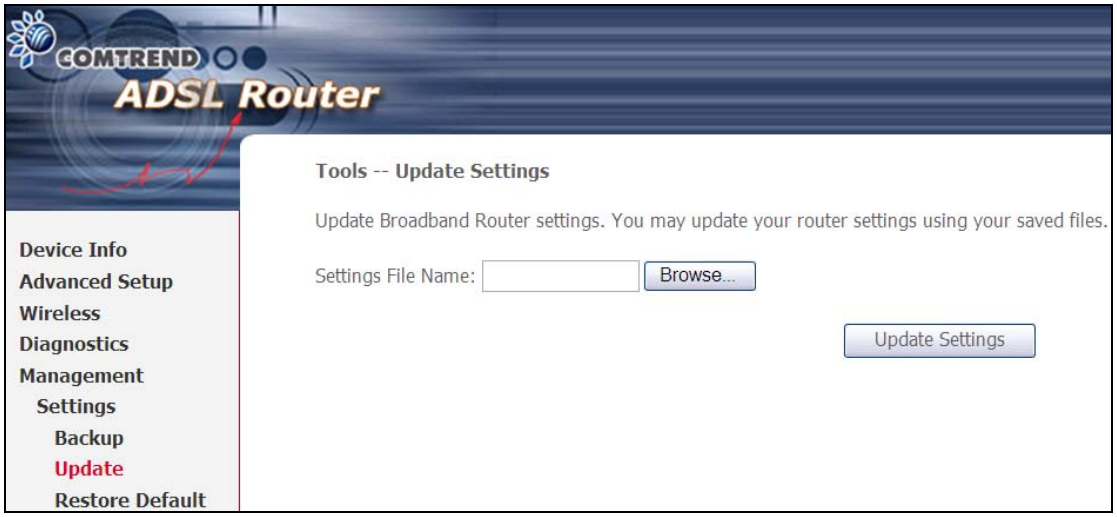
8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.



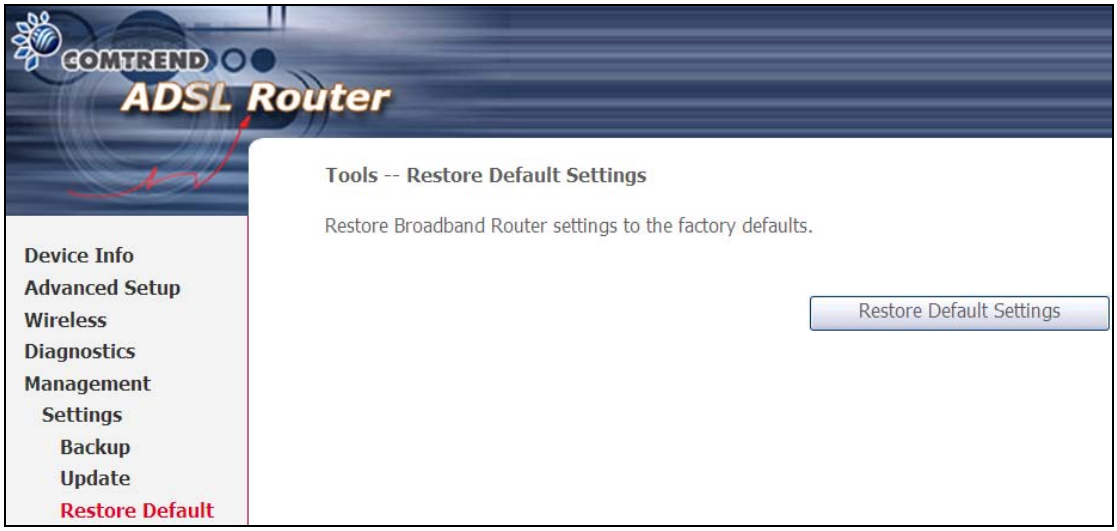
8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse…** to search for the file, then click **Update Settings** to recover settings.

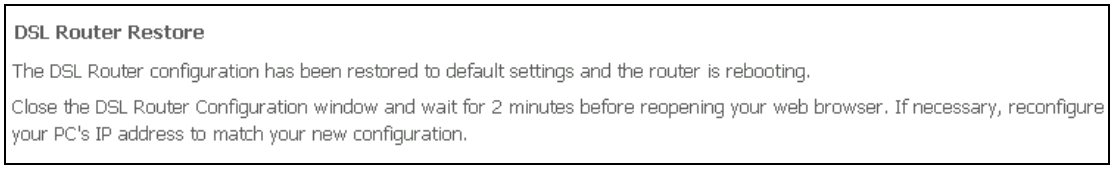


8.1.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.



After **Restore Default Settings** is clicked, the following screen appears.



Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

NOTE:	This entry has the same effect as the **Reset** button. The AR-5382u board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

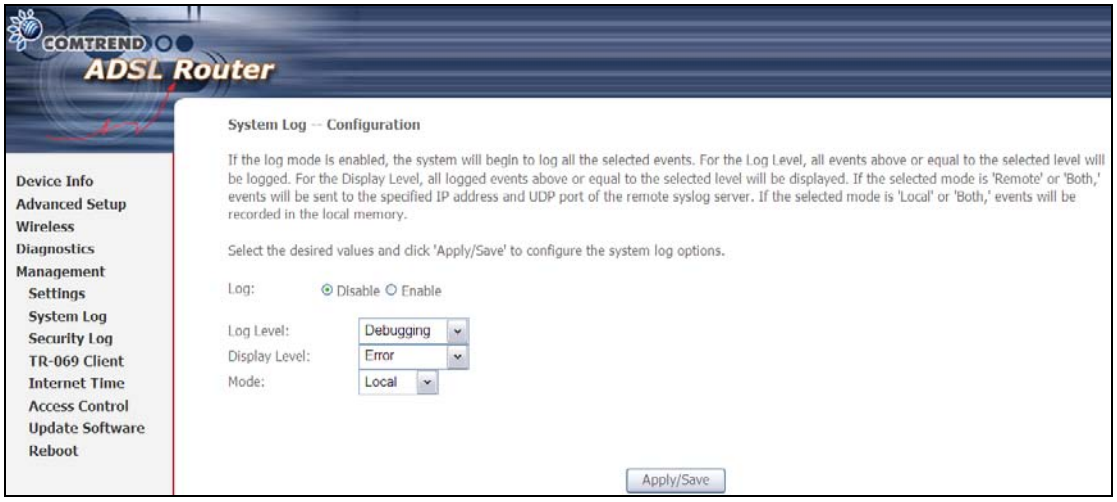
8.2 System Log

This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click **Configure System Log**, as shown below (circled in **Red**).

STEP 2: Select desired options and click **Apply / Save**.

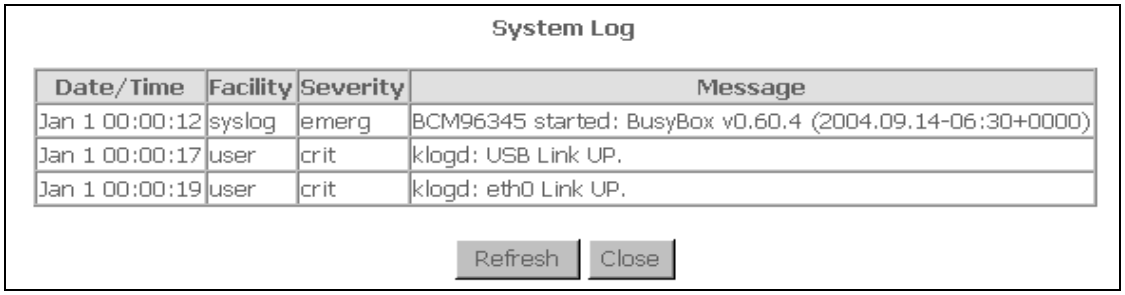


Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the **Enable** radio button and then click **Apply / Save**.

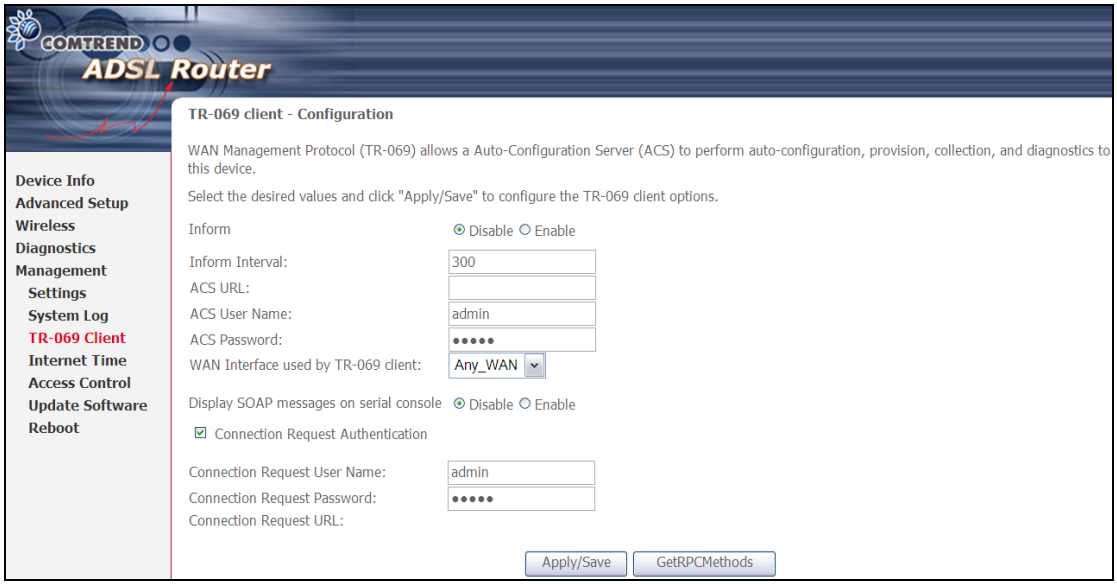
Option	Description
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the AR-5382u SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

STEP 3: Click **View System Log**. The results are displayed as follows.



8.3 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply / Save** to configure TR-069 client options.



The table below is provided for ease of reference.

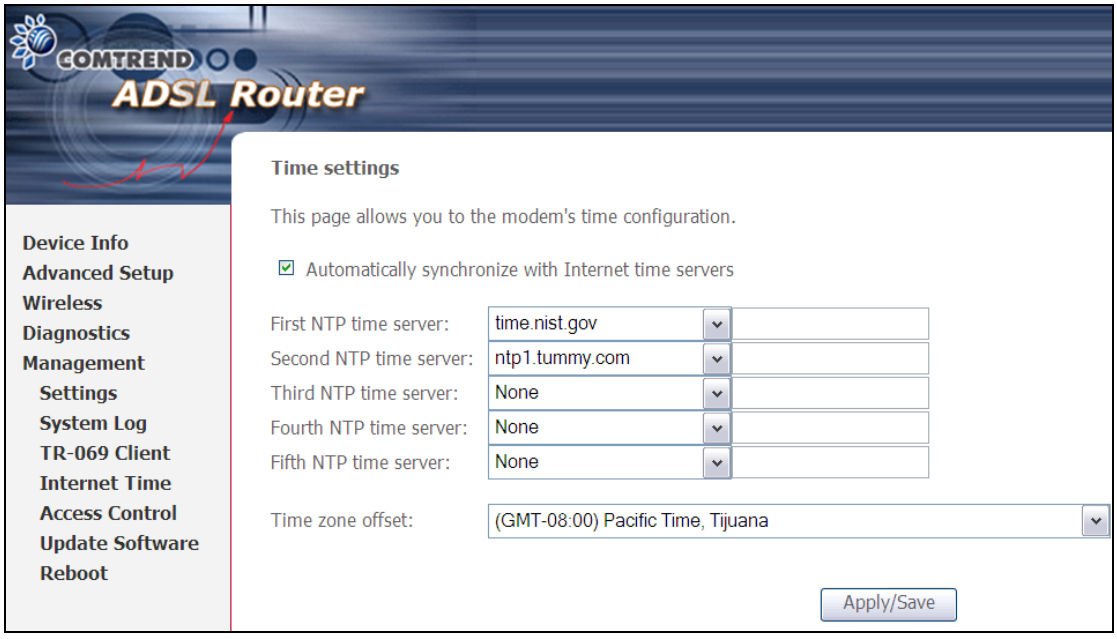
Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Display SOAP messages on serial console	Enable/Disable SOAP messages on serial console. This option is used for advanced troubleshooting of the device.

Option	Description
Connection Request	
Authorization	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to AR-5382u.

The **Get RPC Methods** button forces the CPE to establish an immediate connection to the ACS. This may be used to discover the set of methods supported by the ACS or CPE. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods.

8.4 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox ☑, choose your preferred time server(s), select the correct time zone offset, and click **Save / Apply**.



NOTE: Internet Time must be activated to use Parental Control.
In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

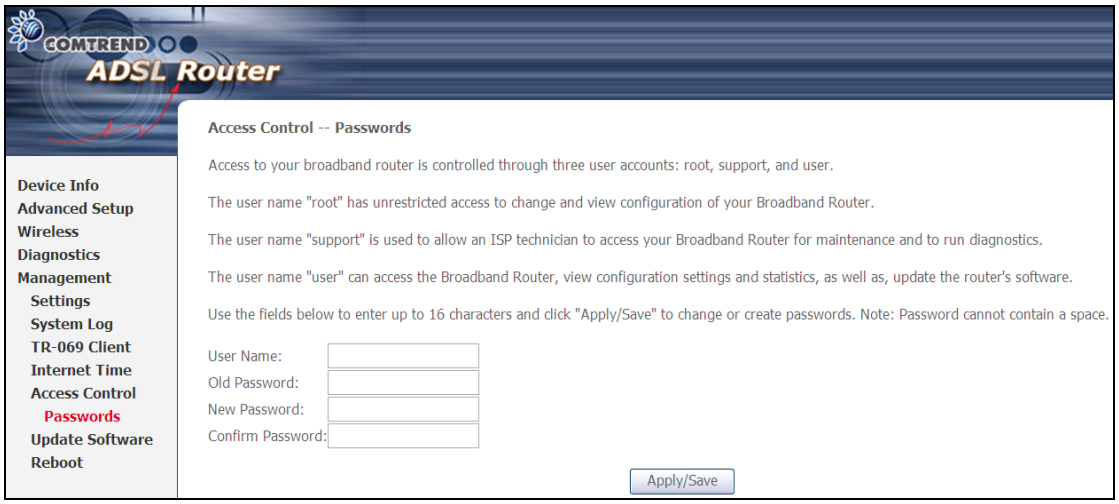
8.5 Access Control

8.5.1 Passwords

This screen is used to configure the user account access passwords for the device. Access to the AR-5382u is controlled through the following three user accounts:

- **root** - unrestricted access to change and view the configuration.
- **support** - used for remote maintenance and diagnostics of the router
- **user** - can view configuration settings & statistics and update firmware.

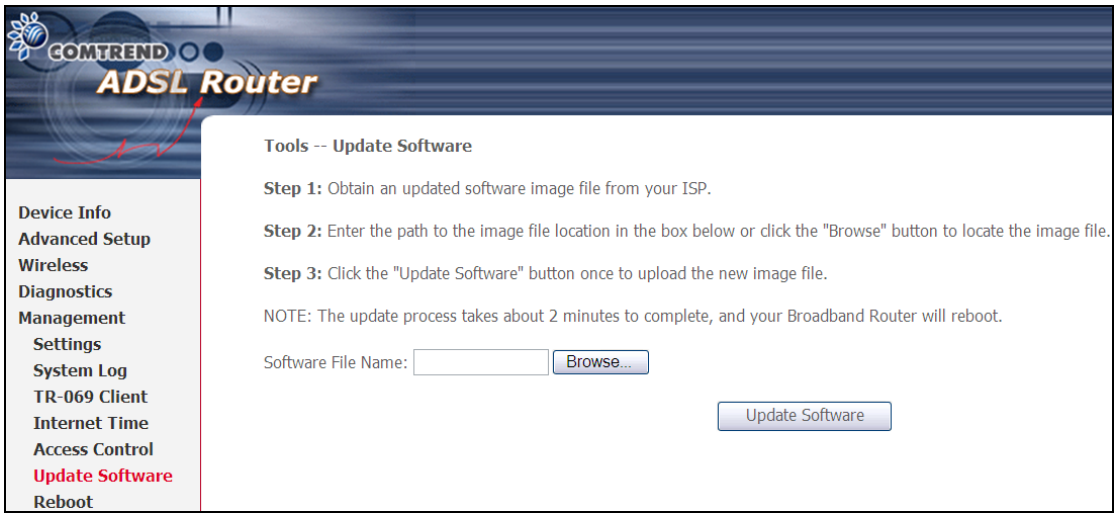
Use the fields below to change password settings. Click **Save / Apply** to continue.



NOTE: Passwords can be up to 16 characters in length.

8.6 Update Software

This option allows for firmware upgrades from a locally stored file.



STEP 1: Obtain an updated software image file from your ISP.

STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 3: Click the **Update Software** button once to upload and install the file.

NOTE:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Chapter 4 Device Information screen with the firmware version installed, to confirm the installation was successful.

8.7 Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.

NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

Appendix A - Firewall

STATEFUL PACKET INSPECTION
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER
These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER
Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Example 1:	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source IP address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. IP Address	: NA
	Dest. Subnet Mask	: NA
	Dest. Port	: NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source IP Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 5060:6060
	Dest. IP Address	: 172.16.13.4
	Dest. Subnet Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER
Helps in setting rules to Allow or Deny packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in Bridge mode. After a Bridge mode connection is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Example 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the AR-5382u, as per chosen days of the week and the chosen times.

Example:

User Name	: FilterJohn
Browser's MAC Address	: 00:25:46:78:63:21
Days of the Week	: Mon, Wed, Fri
Start Blocking Time	: 14:00
End Blocking Time	: 18:00

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B - Pin Assignments

ETHERNET Ports (RJ45)

ETHERNET LAN Ports (10/100Base-T)

Pin	Signal name	Signal definition
1	TXP	Transmit data (positive lead)
2	TXN	Transmit data (negative lead)
3	RXP	Receive data (positive lead)
4	NC	Not used
5	NC	Not used
6	RXN	Receive data (negative lead)
7	NC	Not used
8	NC	Not used

Table 1

Signals for ETHERNET WAN port (10/1001000Base-T)

Pin	Signal name	Signal definition
1	TRD+(0)	Transmit/Receive data 0 (positive lead)
2	TRD-(0)	Transmit/Receive data 0 (negative lead)
3	TRD+(1)	Transmit/Receive data 1 (positive lead)
4	TRD+(2)	Transmit/Receive data 2 (positive lead)
5	TRD-(2)	Transmit/Receive data 2 (negative lead)
6	TRD-(1)	Transmit/Receive data 1 (negative lead)
7	TRD+(3)	Transmit/Receive data 3 (positive lead)
8	TRD-(3)	Transmit/Receive data 3 (negative lead)

Table 2

Appendix C - Specifications

Hardware Interface

- RJ-11 X 1 for ADSL
- RJ-45 X 4 for LAN (10/100 Base-T auto-sense)
- Reset Button X 1
- WPS Button X 1
- Wi-Fi On/Off Button X 1
- Power Switch X 1
- USB Host X 1
- Wi-Fi internal Antenna X2

WAN Interface

- ADSL2+ Downstream : 24 Mbps Upstream : 1.3 Mbps
- ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, AnnexM
- ADSL2 Downstream : 12 Mbps Upstream : 1.3 Mbps

LAN Interface

- Standard IEEE 802.3, IEEE 802.3u
- MDI/MDX support Yes
- 10/100 BaseT Auto-sense

Wireless Interface

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption/ WPA/WPA2 encryption
- 11 Channels (US, Canada)/ 13 Channels (Europe)/ 14 Channels (Japan)
- Up to 300Mbps data rate
- WPA/WPA2 Yes
- IEEE 802.1x Yes
- Afterburner mode (Turbo mode) Yes (this feature is optional)
- RF operating Frequency 2.412-2.497GHz (Generic, 2.4GHz ISM Band),
- 2.400-2.4835GHz (Egypt, 2.4GHz ISM Band)
- WMM Yes

ATM Attribtues

- RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Route; RFC 2516 (PPPoE); RFC 1577 (IPoA), Annex M
- Support PVCs 16
- AAL type AAL5
- ATM service class UBR/CBR/VBR
- ATM UNI support UNI3.1/4.0
- OAM F4/F5 Yes

Management

- Compliant with TR-069/TR-098/TR-111 remote management protocols, SNMP, Telnet, Web-based management, Configuration backup and restoration,
- Software upgrade via HTTP / TFTP / FTP server

Bridge Functions

- Transparent bridging and learning
- VLAN support
- Spanning Tree Algorithm
- IGMP Proxy

Routing Functions

Static route, RIP, and RIPv2, NAT/PAT, DHCP Server/DHCP Relay/DHCP Client, DNS Proxy, ARP

Security Functions

- PAP, CHAP, TCP/IP/Port filtering rules
- Port triggering/Forwarding,
- Packet and MAC address filtering, Access control, SSH access

QoS

- L3 policy-based QoS, IP QoS, ToS

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc.

Power Supply .....Input: 100 - 240 Vac
Output: 12 Vdc / 1 A

Environment Condition

Operating temperature .....0 ~ 50 degrees Celsius
Relative humidity .....5 ~ 95% (non-condensing)

Certifications..... CE

Kit Weight

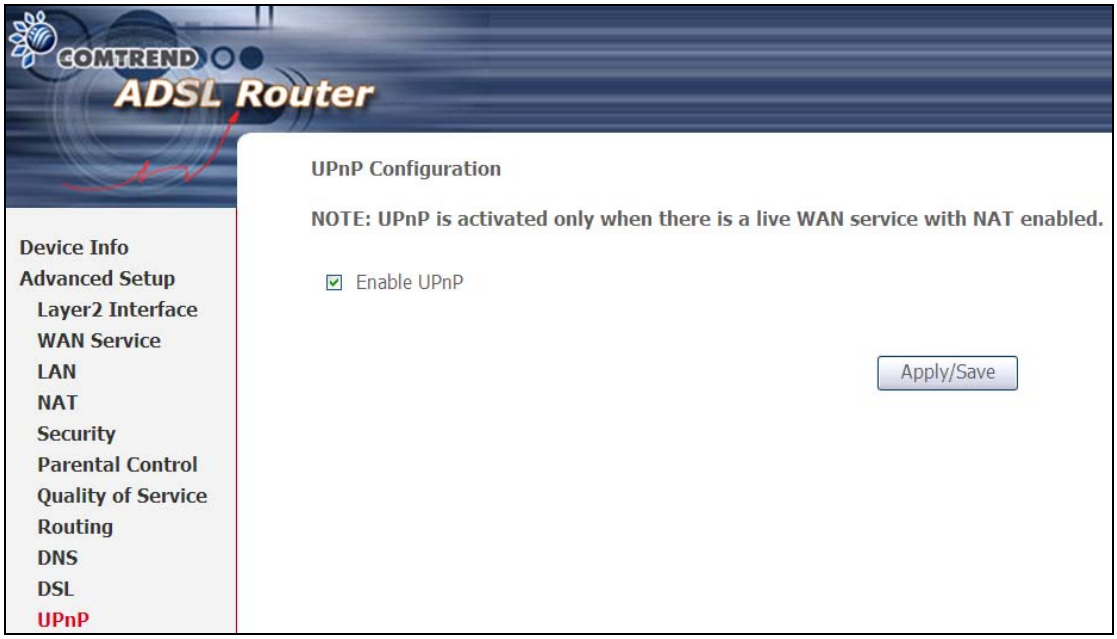
(1*AR-5382u, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM) = 0.5 kg

NOTE: Specifications are subject to change without notice

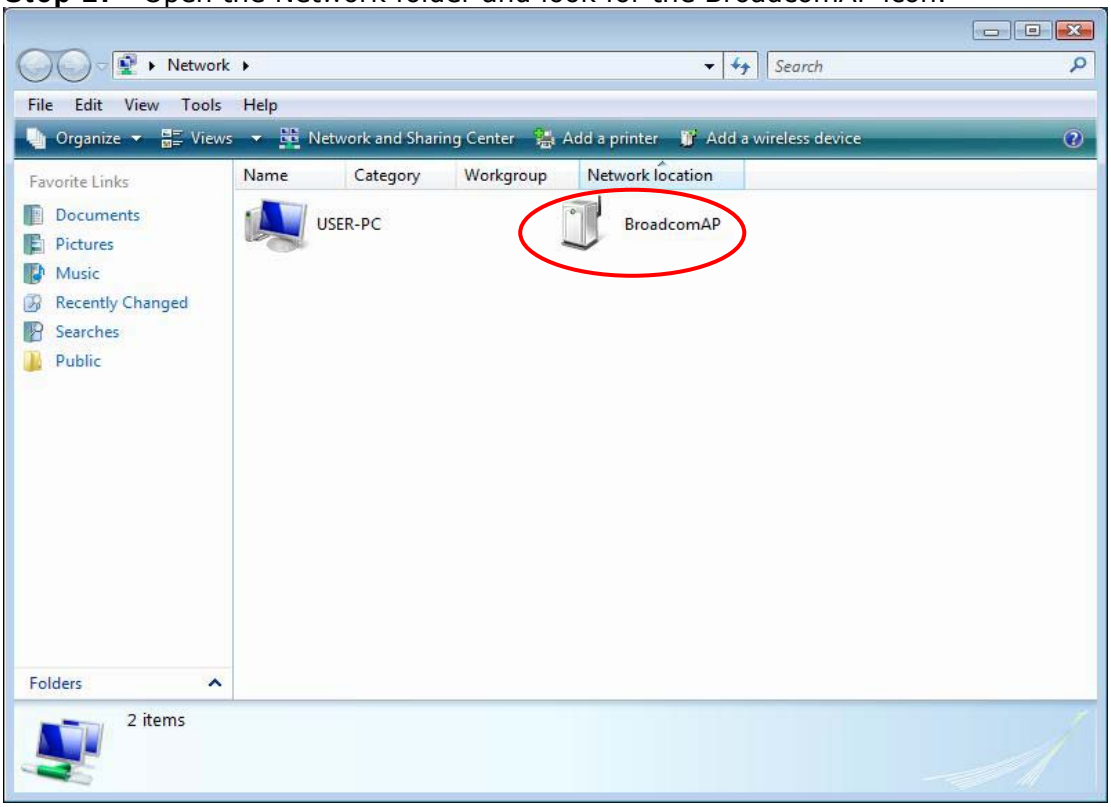
Appendix D - WPS External Registrar

Follow these steps to add an external registrar using the web user interface (WUI) on a personal computer running the Windows Vista operating system:

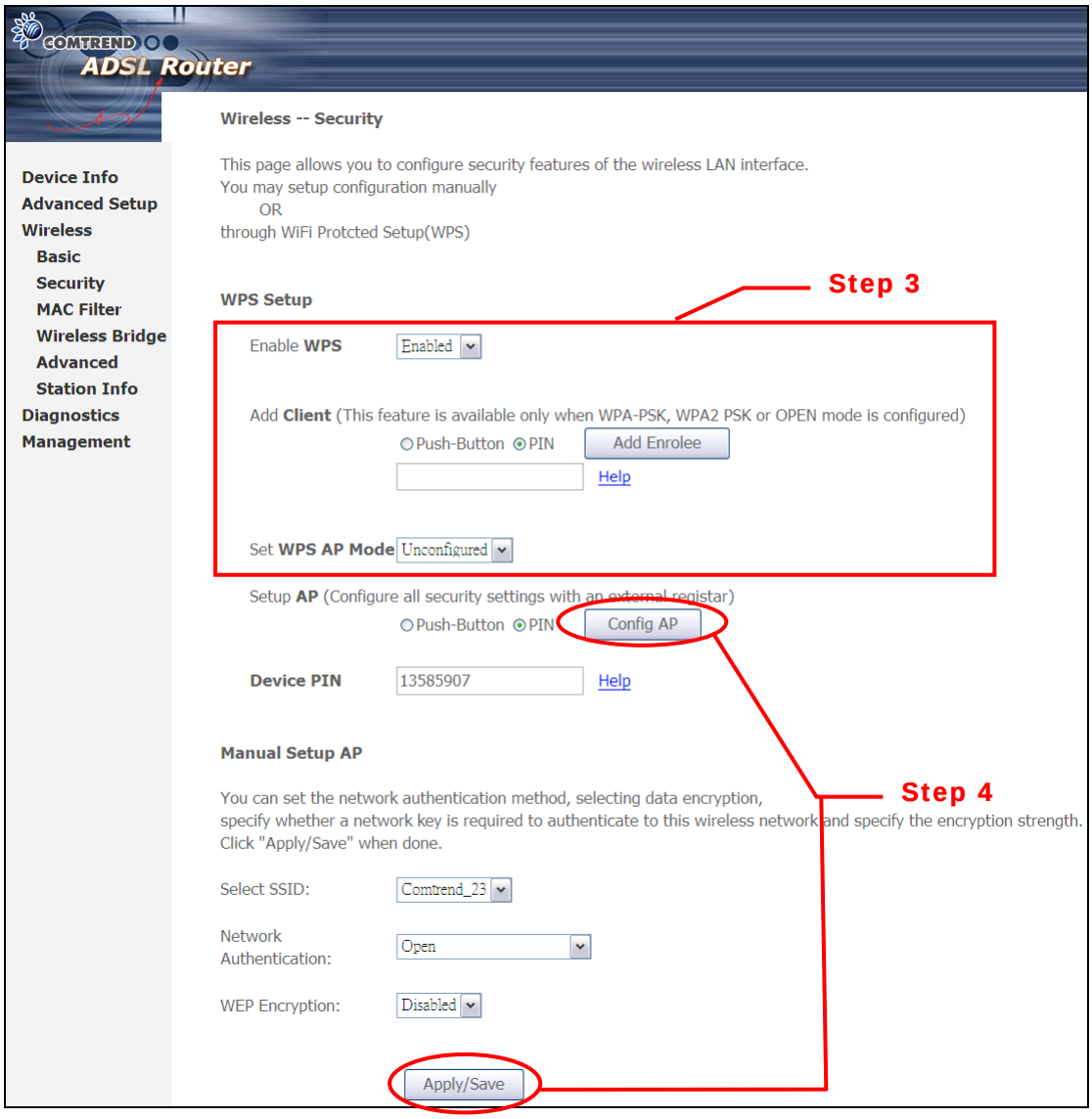
Step 1: Enable Upnp on the Advanced Setup.



Step 2: Open the Network folder and look for the BroadcomAP icon.

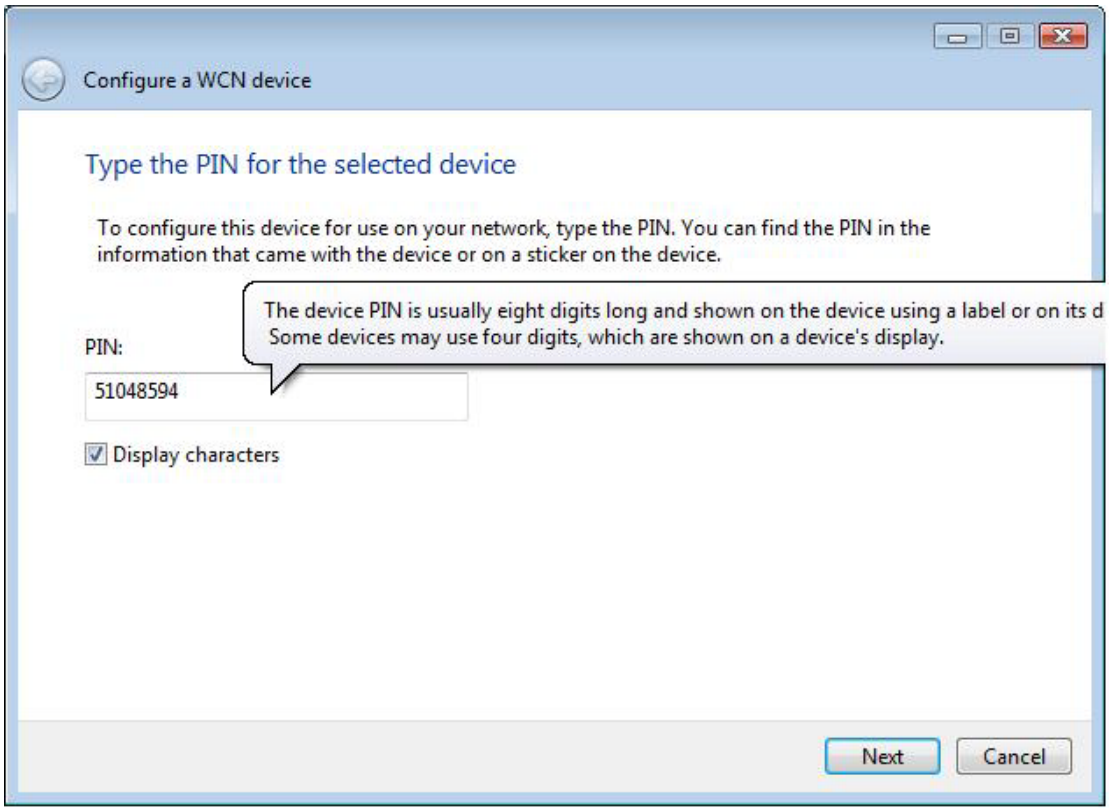


Step 3: On the Wireless → Security screen, enable WPS by selecting **Enabled** from the drop down list box and set the WPS AP Mode to Unconfigured.

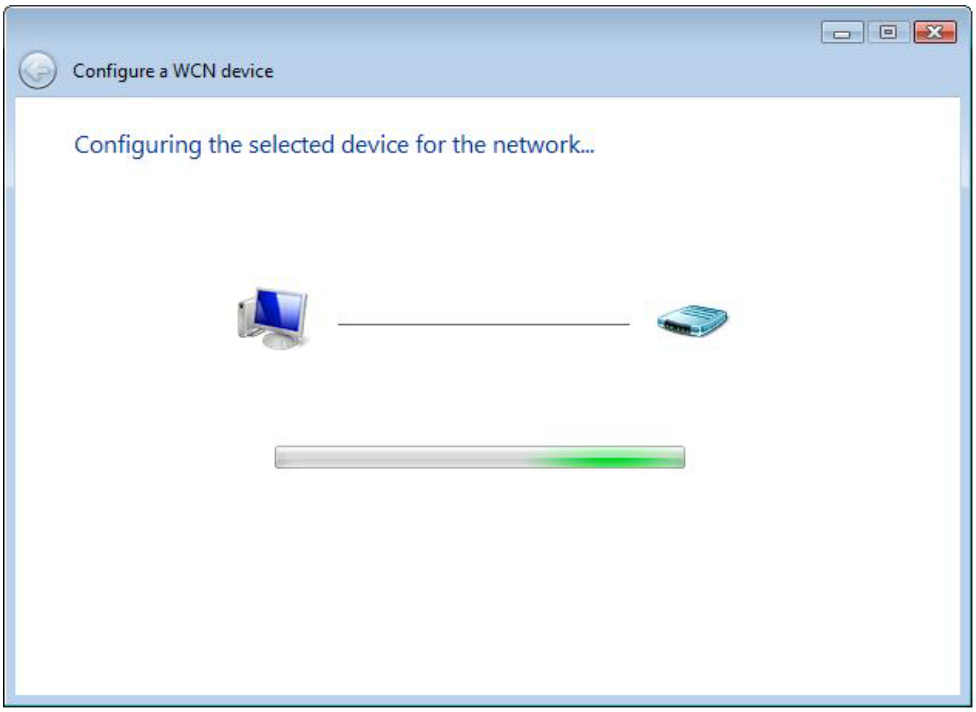


Step 4: Click the **Save / Apply** button at the bottom of the screen. The screen will go blank while the router applies the new Wireless settings. When the screen returns, press the **Config AP** button, as shown above.

Step 5: Now return to the Network folder and click the BroadcomAP icon. A dialog box will appear asking for the Device PIN number. Enter the Device PIN as shown on the Wireless → Security screen. Click **Next**.



Step 6: Windows Vista will attempt to configure the wireless security settings.



Step 7: If successful, the security settings will match those in Windows Vista.

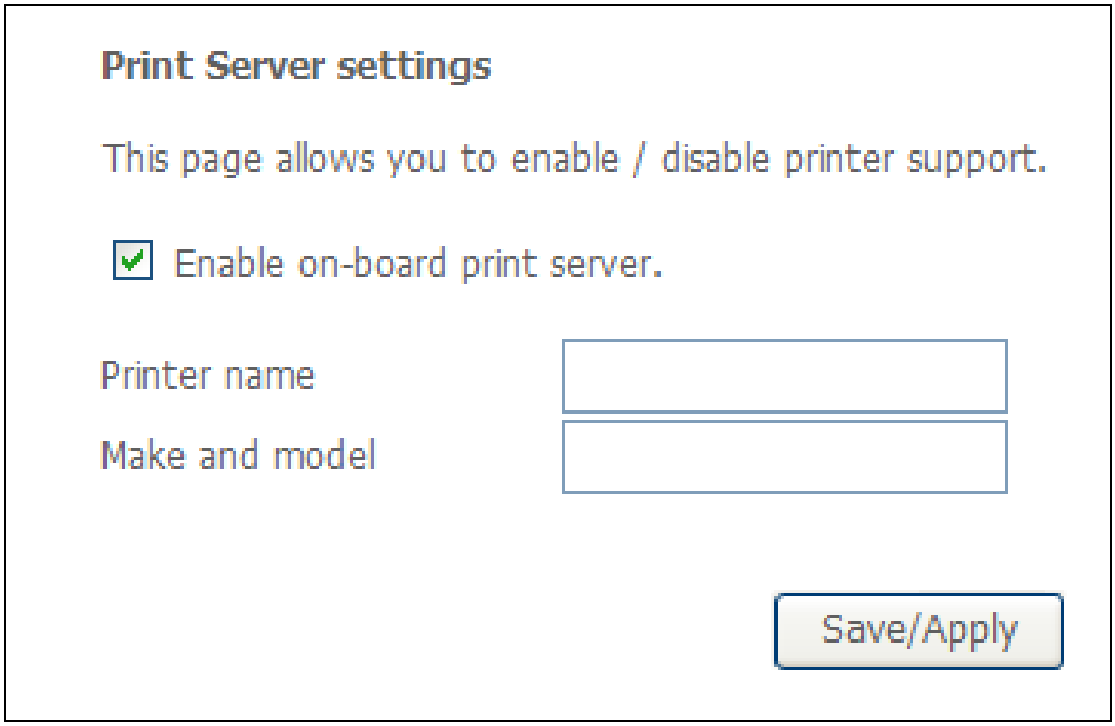
Appendix E - Printer Server

These steps explain the procedure for enabling the Printer Server.

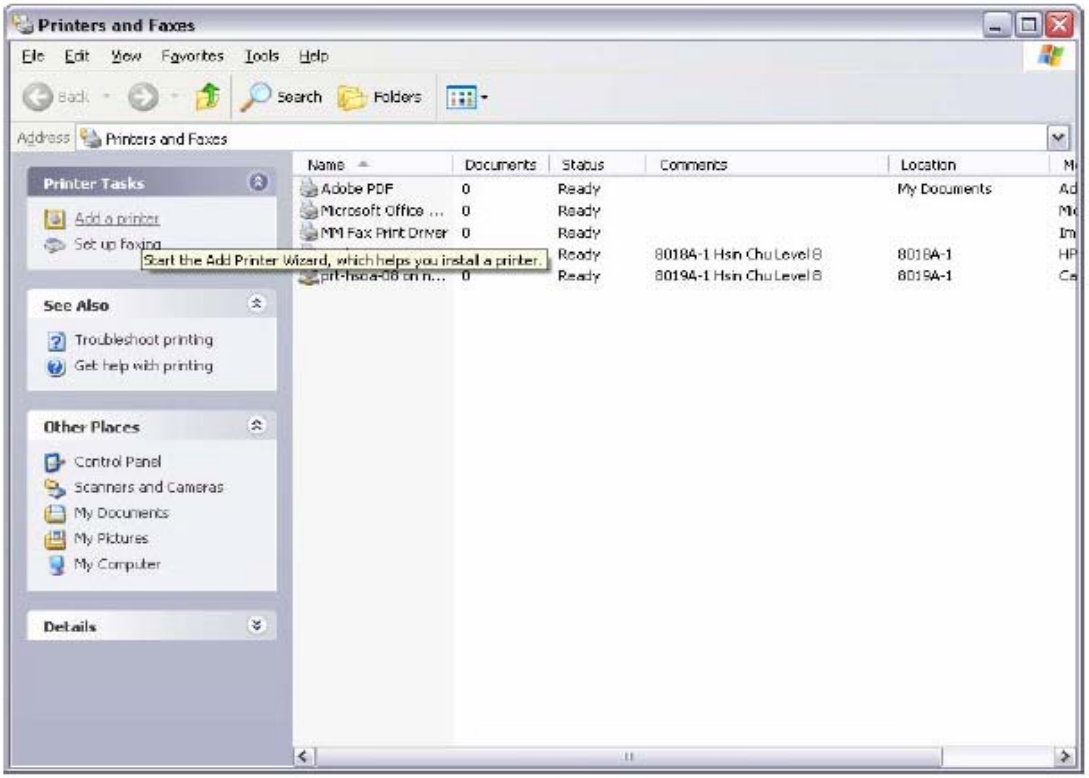
NOTE:	This function only applies to models with an USB host port.

STEP 1: Enable Print Server from Web User Interface. Select Enable on-board print server checkbox ☑ and enter Printer name and Make and model

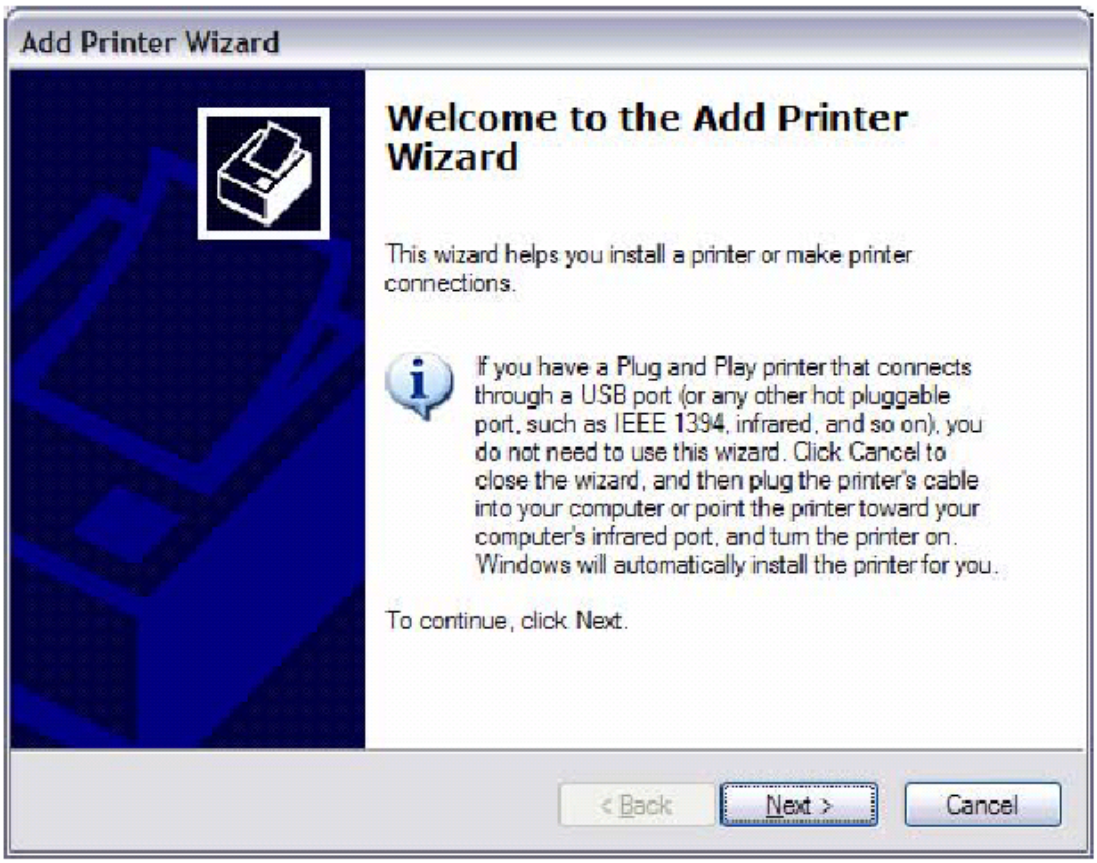
NOTE:	The **Printer name** can be any text string up to 40 characters. The **Make and model** can be any text string up to 128 characters.



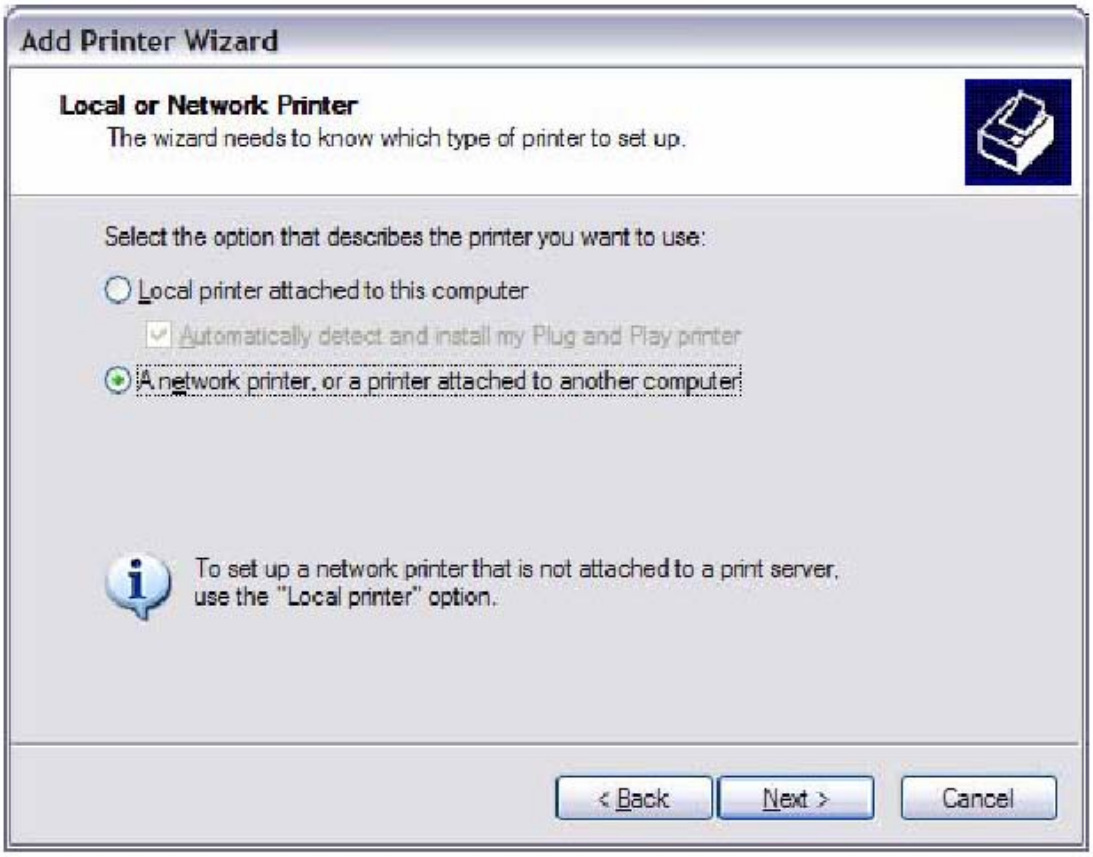
STEP 2: Go to the **Printers and Faxes** application in the **Control Panel** and select the **Add a printer** function (as located on the side menu below).



STEP 3: Click **Next** to continue when you see the dialog box below.



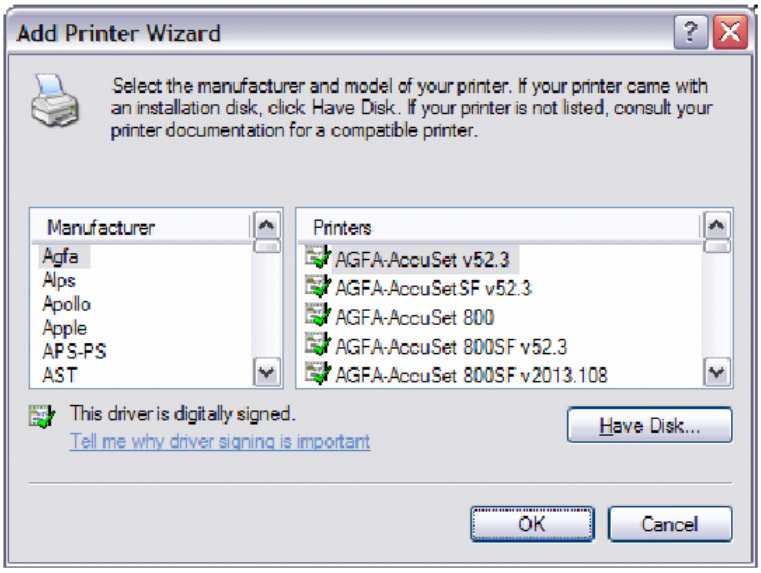
STEP 4: Select **Network Printer** and click **Next**.



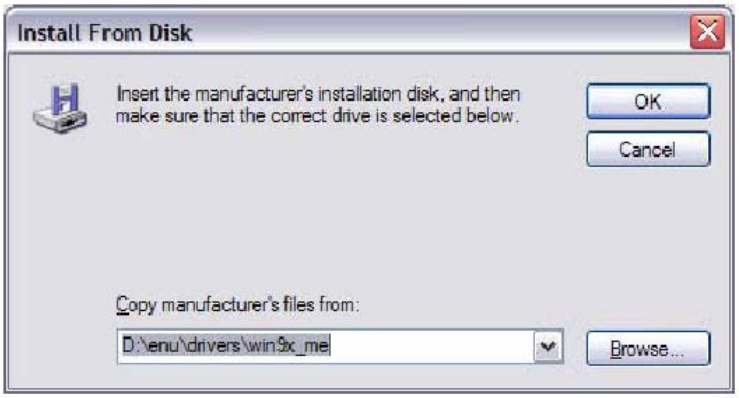
STEP 5: Select Connect to a printer on the Internet and enter your printer link. (e.g. http://192.168.1.1:631/printers/hp3845) and click **Next**.

NOTE:	The printer name must be the same name entered in the ADSL modem WEB UI "printer server setting" as in step 1.

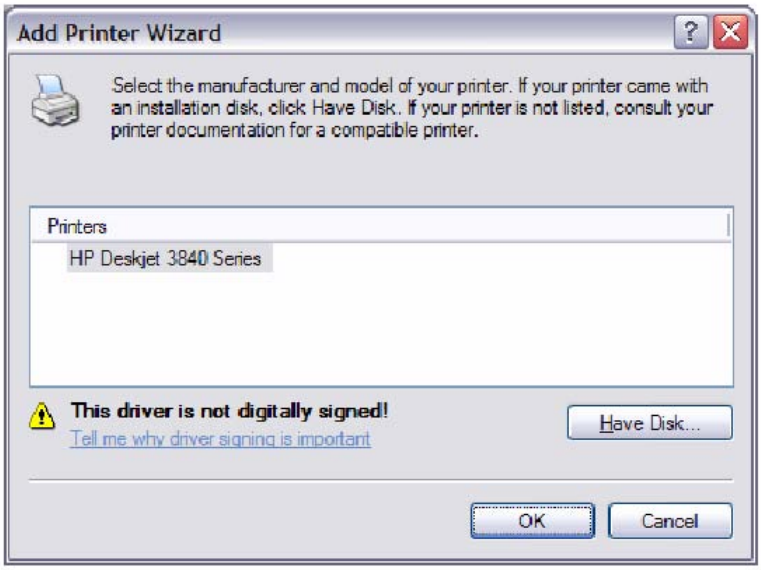
STEP 6: Click **Have Disk** and insert the printer driver CD.



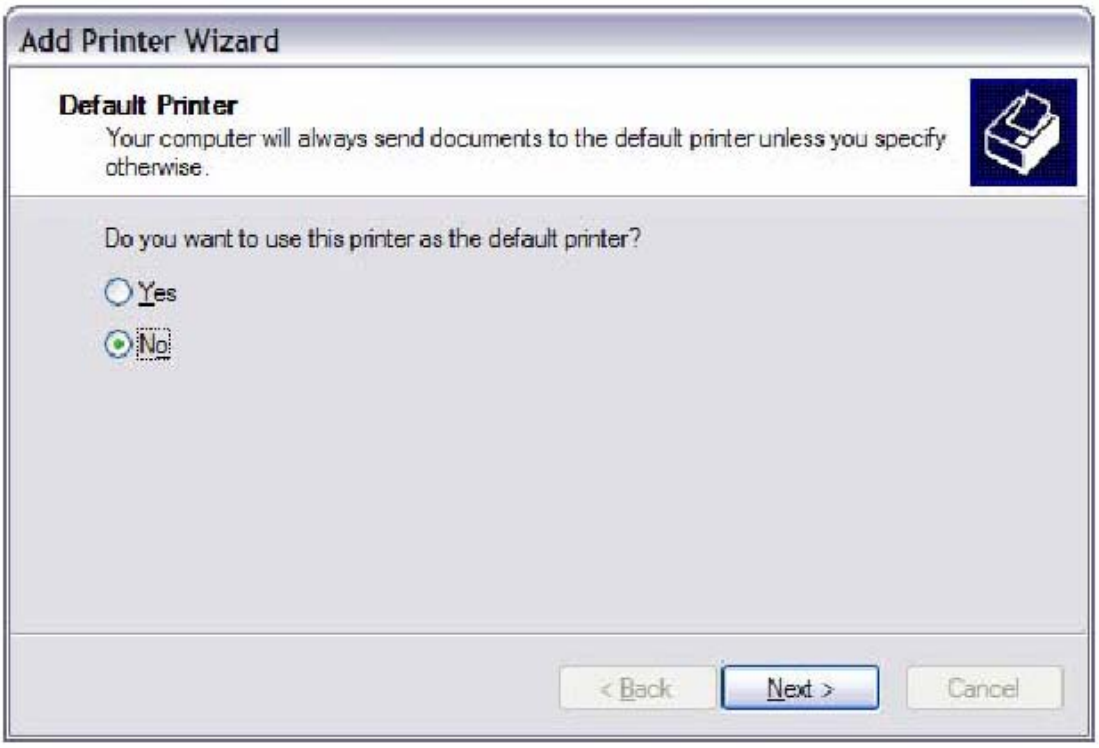
STEP 7: Select driver file directory on CD-ROM and click **OK**.



STEP 8: Once the printer name appears, click **OK**.

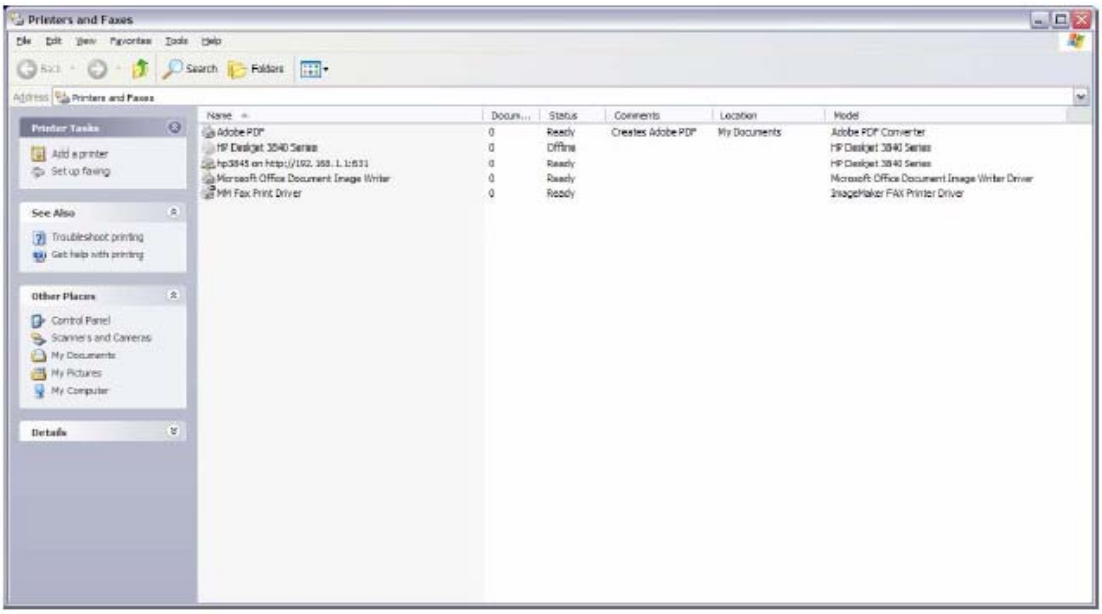


STEP 9: Choose **Yes** or **No** for default printer setting and click **Next.**



STEP 10: Click Finish.

STEP 11: Check the status of printer from Windows Control Panel, printer window. Status should show as **Ready**.



Appendix F - Connection Setup

Creating a WAN connection is a two-stage process.

1 - Setup a Layer 2 Interface (ATM or PTM).
2 - Add a WAN connection to the Layer 2 Interface.

The following sections describe each stage in turn.

F1 ~ Layer 2 Interfaces

Every layer2 interface operates in one of three modes: Default or VLAN Mux. A short introduction to each of these three modes is included below for reference. It is important to understand the differences between these connection modes, as they determine the number and types of connections that may be configured.

DEFAULT MODE

In this mode there is a 1:1 relationship between interfaces and WAN connections, in that an interface in default mode supports just one connection. However, unlike the multiple connection modes described below, it supports all five connection types. The figure below shows the five connection types available in ATM default mode.
Note: EoA Link Type is for PPPoE, IPoE, and Bridge.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			☐
atm2	1	35	Path0	UBR	PPPoA	DefaultMode	Enabled	SP			☐
ipoa0	3	35	Path0	UBR	IPoA	DefaultMode	Enabled	SP			☐

VLAN MUX MODE

This mode uses VLAN tags to allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not. The figure below shows multiple connections over a single VLAN Mux interface.

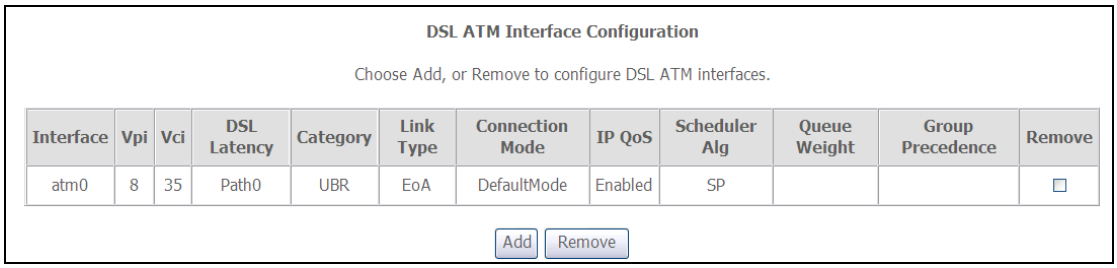
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Remove	Edit
ipoa0	ipoa_0_3_35	IPoA	N/A	N/A	Disabled	Disabled	Disabled	☐	Edit
ppp0	internet	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	☐	Edit
pppoa1	pppoa_0_1_35	PPPoA	N/A	N/A	Disabled	Disabled	Disabled	☐	Edit

F1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE:	The AR-5382u supports up to 16 ATM interfaces.

STEP 1: Go to Advanced Setup → Layer2 Interface → ATM Interface.

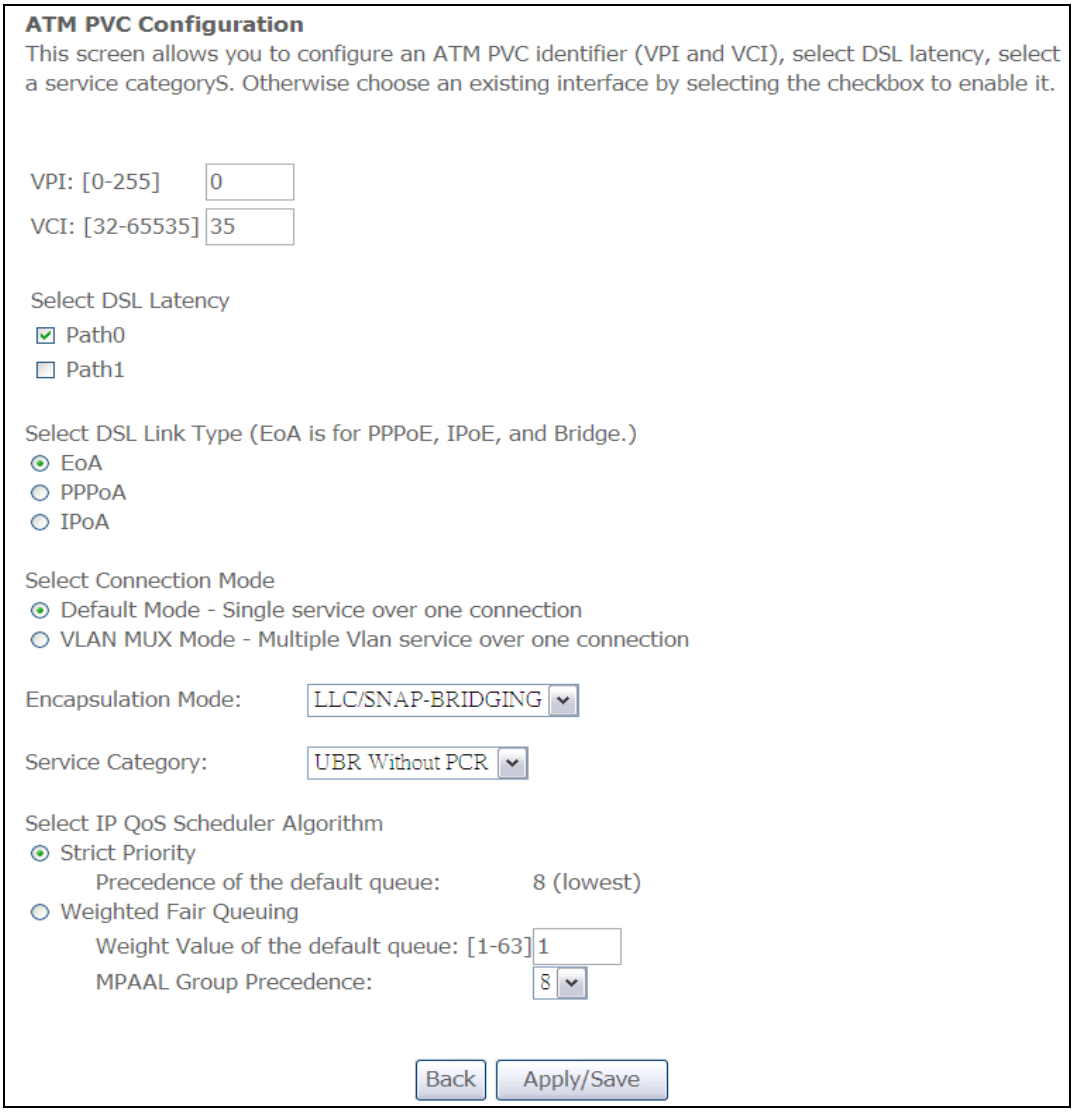


This table is provided here for ease of reference.

Heading	**Description**
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → port ID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	ATM service category
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection
IP QoS	Quality of Service (IP QoS) status
Scheduler Alg	The algorithm used to schedule the data in the queues. There are two algorithms to choose, strict priority and weighted fair queueing.
Queue Weight	The weight of the specified queue. This value decides how much data can be sent in every cycle for this queue.
Group Precedence	The precedence of the specified group. This value decides the order of sending data for this queue in this group for every cycle regardless of FIFO. The default queue precedence (strict priority) is 8(lowest).
Remove	Select items for removal

STEP 2: Click **Add** to proceed to the next screen.

NOTE:	To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.



There are many settings here including: VPI/VCI, DSL Latency, DSL Link Type, Encapsulation Mode, Service Category, Connection Mode and Quality of Service.

The table below shows xDSL Link Type availability with each Connection Mode.

	xDSL Link Type		
Connection Mode	EoA*	PPPoA	IPoA
Default Mode	OK	OK	OK
VLAN Mux Mode	OK	X	X

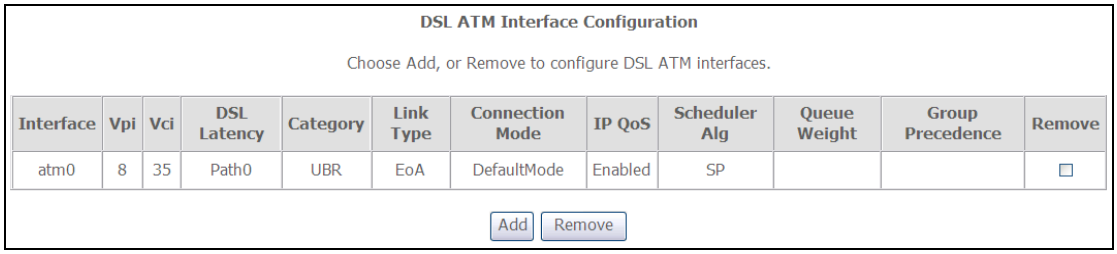
* EoA includes PPPoE, IPoE, and Bridge link types.

Here are the available encapsulations for each xDSL Link Type:

- EoA- LLC/SNAP-BRIDGING, VC/MUX
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- IPoA- LLC/SNAP-ROUTING, VC MUX

STEP 3: Click **Apply / Save** to confirm your choices.

On the next screen, check that the ATM interface is added to the list. For example, an ATM interface on PVC 0/35 in Default Mode with an EoA Link type is shown below.



To add a WAN connection, go to section G2 ~ WAN Connections.

This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	ATM service category
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. MSC Mode – Multiple Services over one interface.
IP QoS	Quality of Service (QoS) status.
Scheduler Alg	The algorithm used to schedule the data in the queues. There are two algorithms to choose, strict priority and weighted fair queueing.
Queue Weight	The weight of the specified queue. This value decides how much data can be sent in every cycle for this queue.
Group Precedence	The precedence of the specified group. This value decides the order of sending data for this queue in this group for every cycle regardless of FIFO. The default queue precedence (strict priority) is 8(lowest).
Remove	Select interfaces to remove.

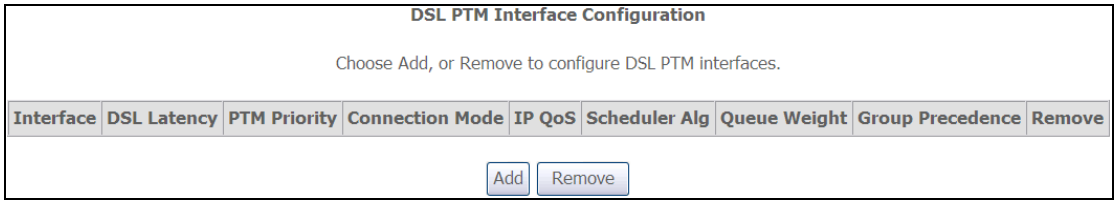
NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

F1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

NOTE: The AR-5382u supports up to four PTM interfaces.

STEP 4: Go to Advanced Setup → Layer2 Interface → PTM Interface.

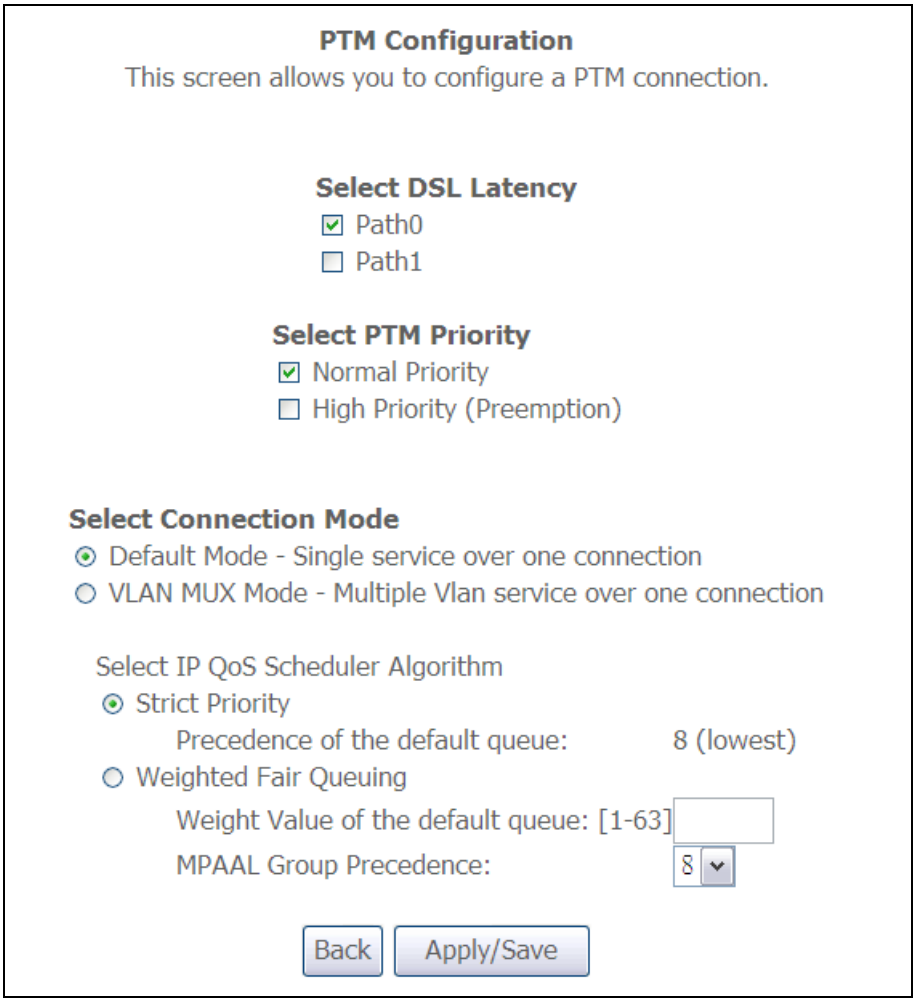


This table is provided here for ease of reference.

Heading	Description
Interface	WAN interface name.
DSL Latency	{Path0} → portID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
PTM Priority	Normal or High Priority (Preemption).
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. MSC Mode – Multiple Services over one interface.
IP QoS	Quality of Service (QoS) status.
Scheduler Alg	The algorithm used to schedule the data in the queues. There are two algorithms to choose, strict priority and weighted fair queueing.
Queue Weight	The weight of the specified queue. This value decides how much data can be sent in every cycle for this queue.
Group Precedence	The precedence of the specified group. This value decides the order of sending data for this queue in this group for every cycle regardless of FIFO. The default queue precedence (strict priority) is 8(lowest).
Remove	Select interfaces to remove.

STEP 5: Click **Add** to proceed to the next screen.

NOTE: To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

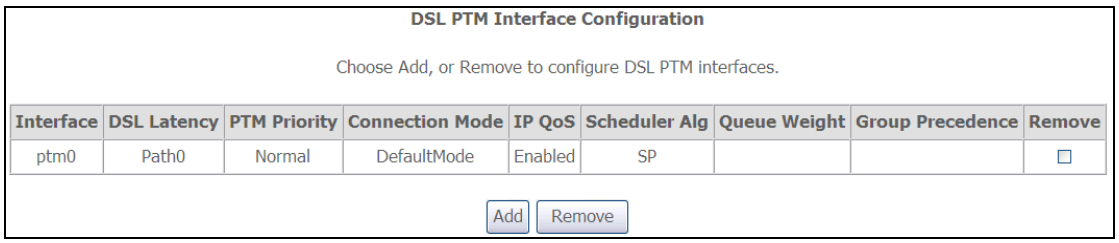


There are many settings that can be configured here including:
DSL Latency, PTM Priority, Connection Mode and Quality of Service.

STEP 6: Click **Apply/Save** to confirm your choices.

On the next screen, check that the PTM interface is added to the list.

For example, an PTM interface in Default Mode is shown below.



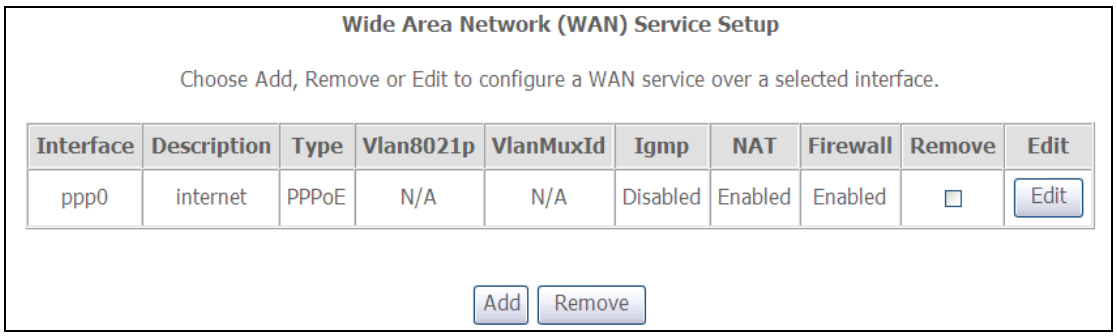
To add a WAN connection, go to section G2 ~ WAN Connections.

F2 ~ WAN Connections

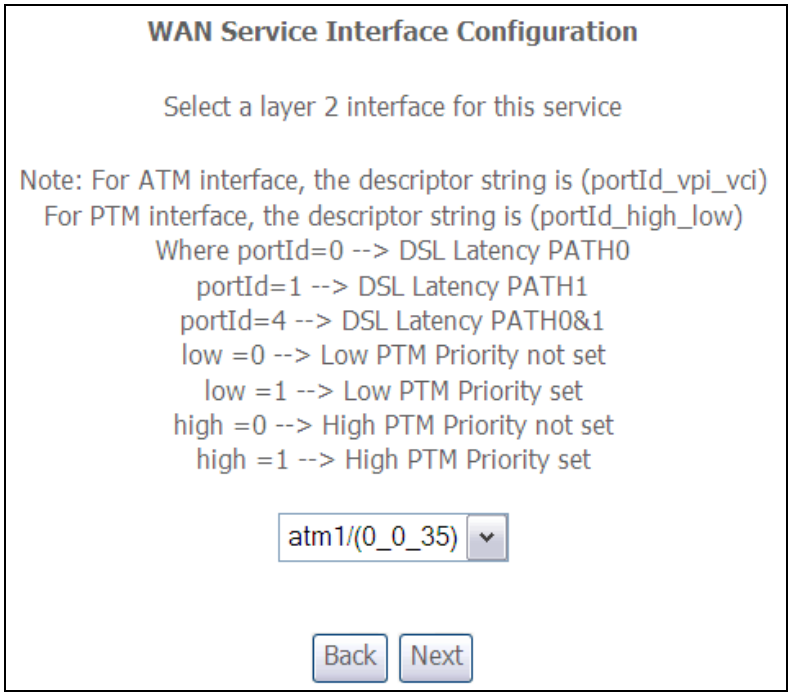
In Default Mode, the AR-5382u supports one WAN connection for each interface, up to a maximum of 8 connections. VLAN Mux and MSC support up to 16 connections.

To setup a WAN connection follow these instructions.

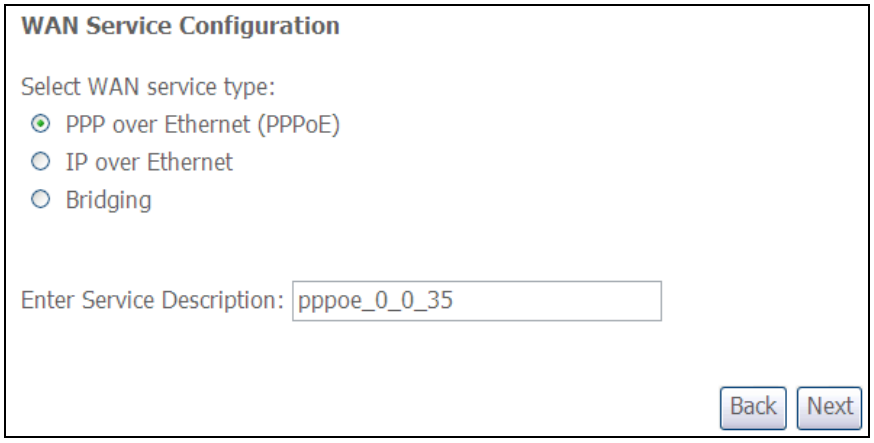
STEP 1: Go to the Advanced Setup → WAN Service screen.



STEP 2: Click **Add** to create a WAN connection. The following screen will display.

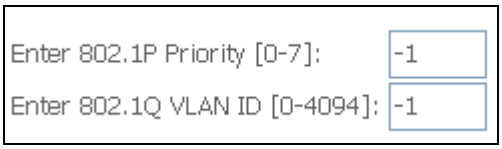


STEP 3: Choose a layer 2 interface from the drop-down box and click **Next**. The WAN Service Configuration screen will display as shown below.



NOTE:	The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.

STEP 4: For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.



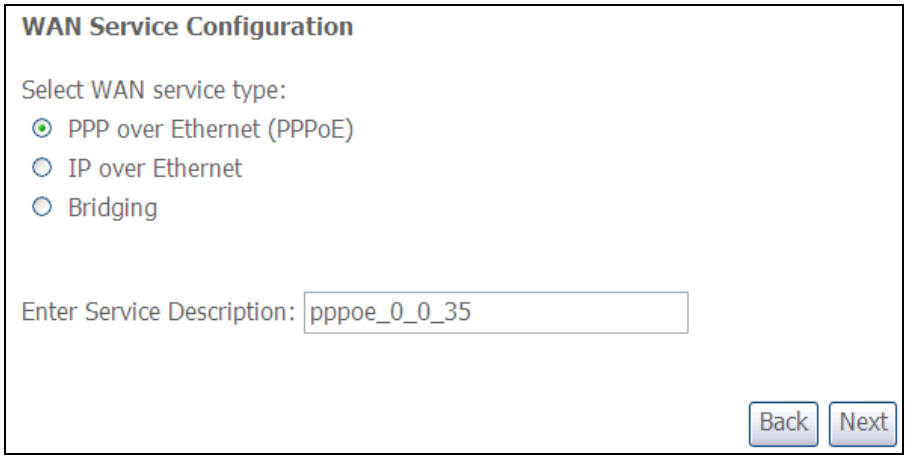
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For F2.1 PPP over ETHERNET (PPPoE), go to page 115.
(2) For F2.2 IP over ETHERNET (IPoE), go to page 120.
(3) For F2.3 Bridging, go to page 123.
(4) For F2.4 PPP over ATM (PPPoA), go to page 124.
(5) For F2.5 IP over ATM (IPoA), go to page 128.

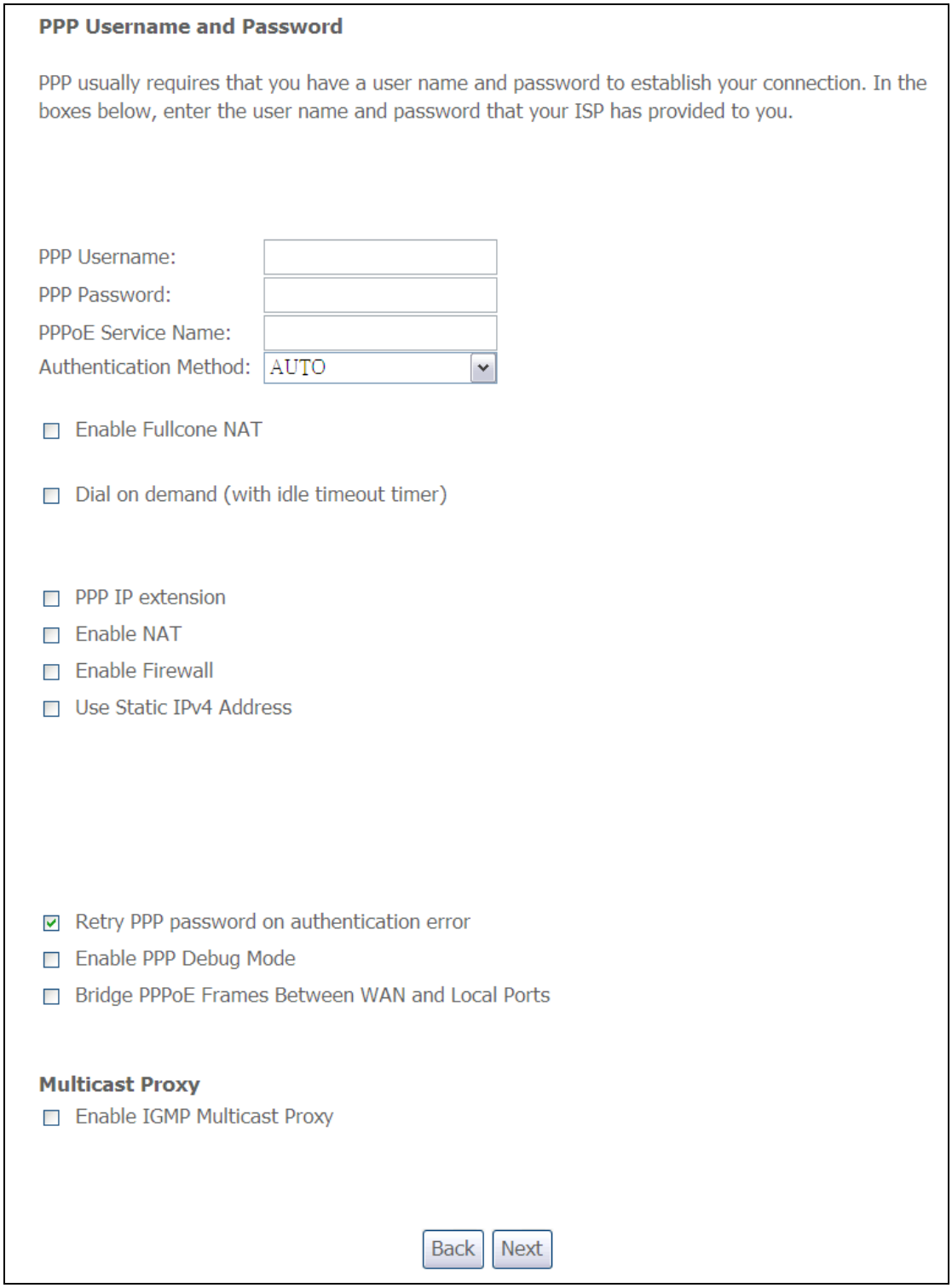
The subsections that follow continue the WAN service setup procedure.

F2.1 PPP over ETHERNET (PPPoE)

STEP 1: Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.



STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.



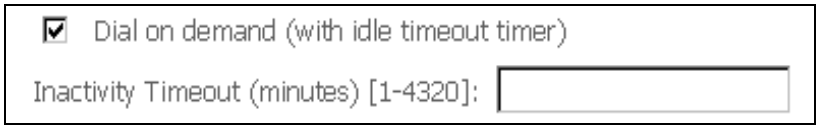
The settings shown above are described below.

PPP SETTINGS

The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The AR-5382u can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- Allows only one PC on the LAN.
- Disables NAT and Firewall.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv4 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in 3.2 IP Configuration.

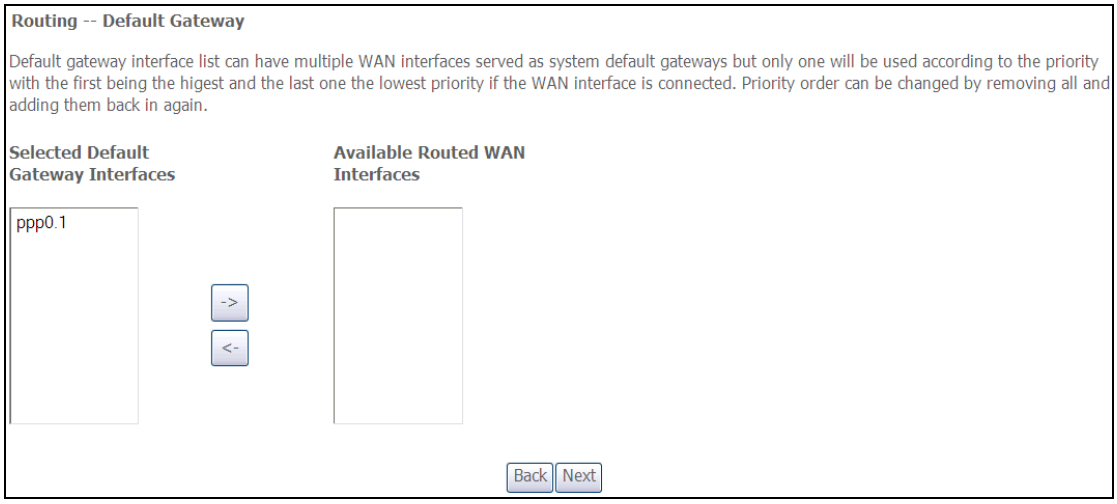
Retry PPP password on authentication error
This feature will redirect users to another WEB page for PPP username/password re-entry if PPP authentication fails.
Tick the box to select.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The AR-5382u supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

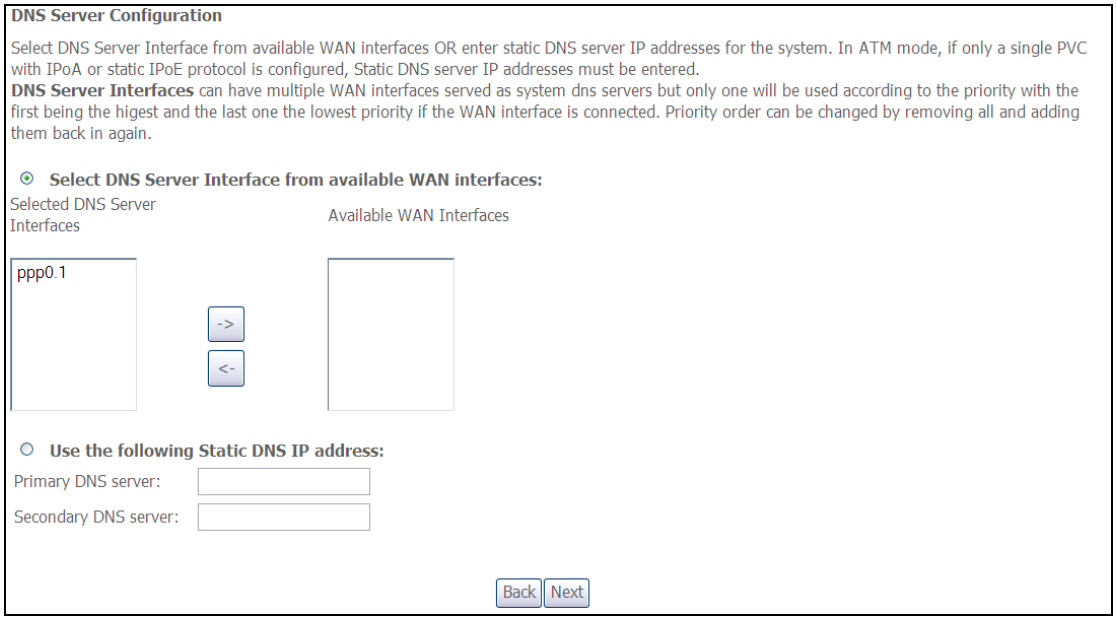
STEP 3: Choose an interface to be the default gateway.



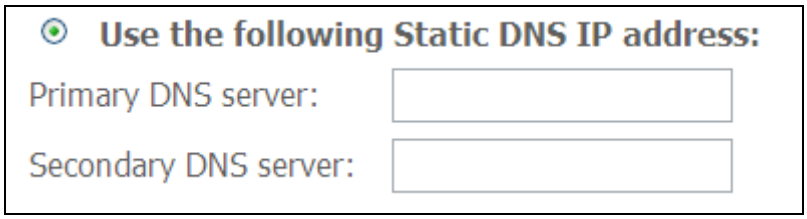
Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. Click **Next** to continue or click **Back** to return to the previous step.

Note: In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

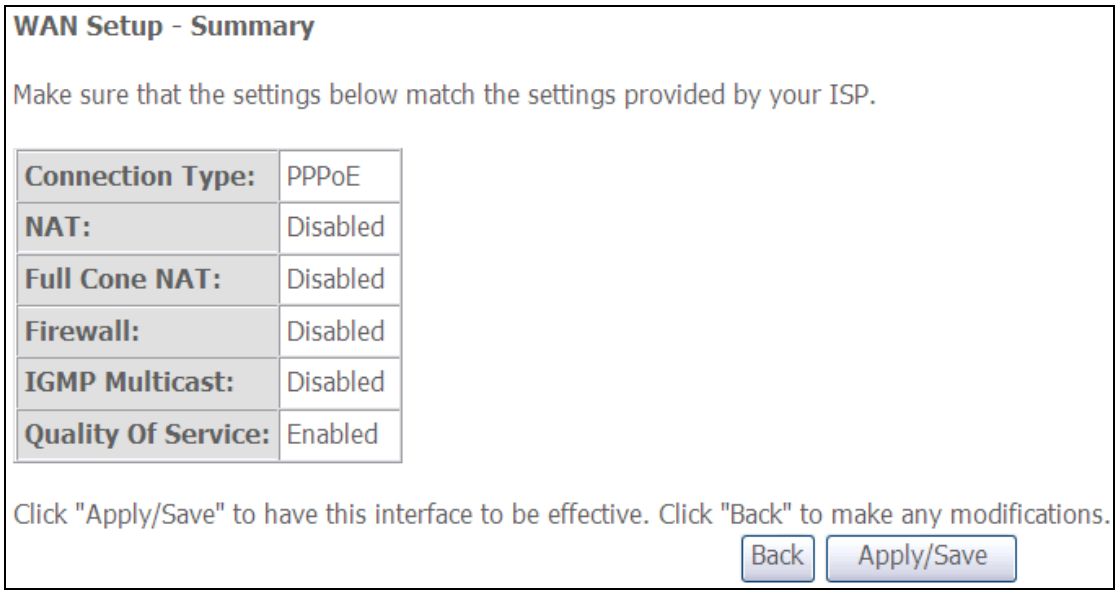


STEP 5: Set the IP address to which the CPE will use to relay DNS query.



Click **Next** to continue or click **Back** to return to the previous step.

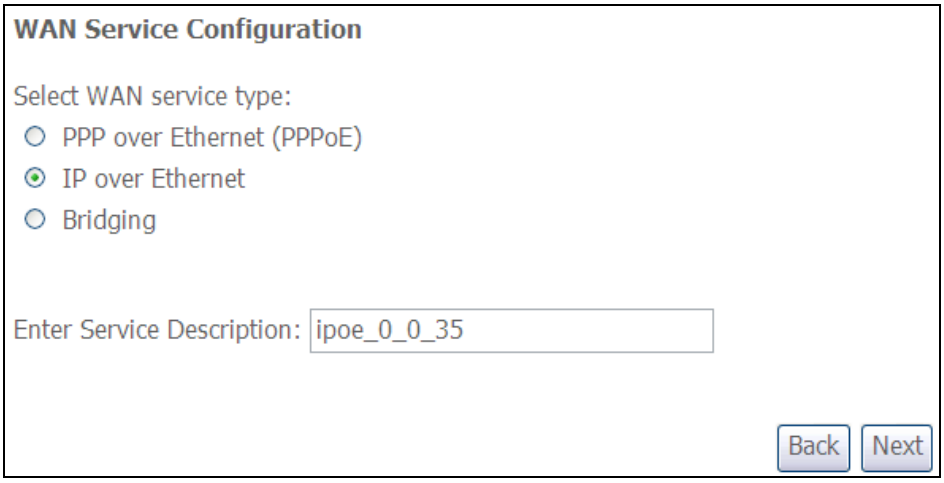
STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.



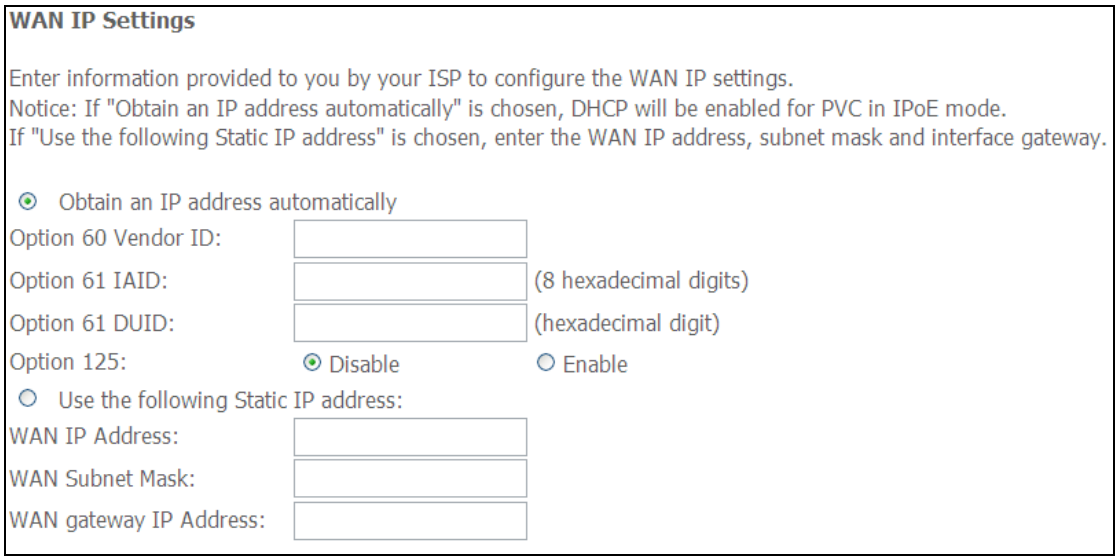
After clicking **Apply / Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

F2.2 IP over ETHERNET (IPoE)

STEP 1: Select the IP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.



STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the **Static IP address** method to assign WAN IP address, Subnet Mask and Default Gateway manually.



Click **Next** to continue or click **Back** to return to the previous step.

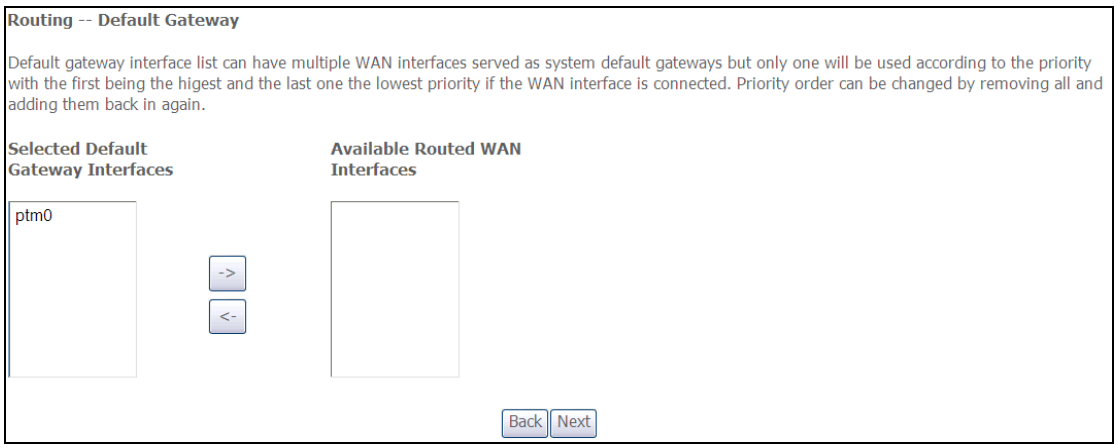
STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

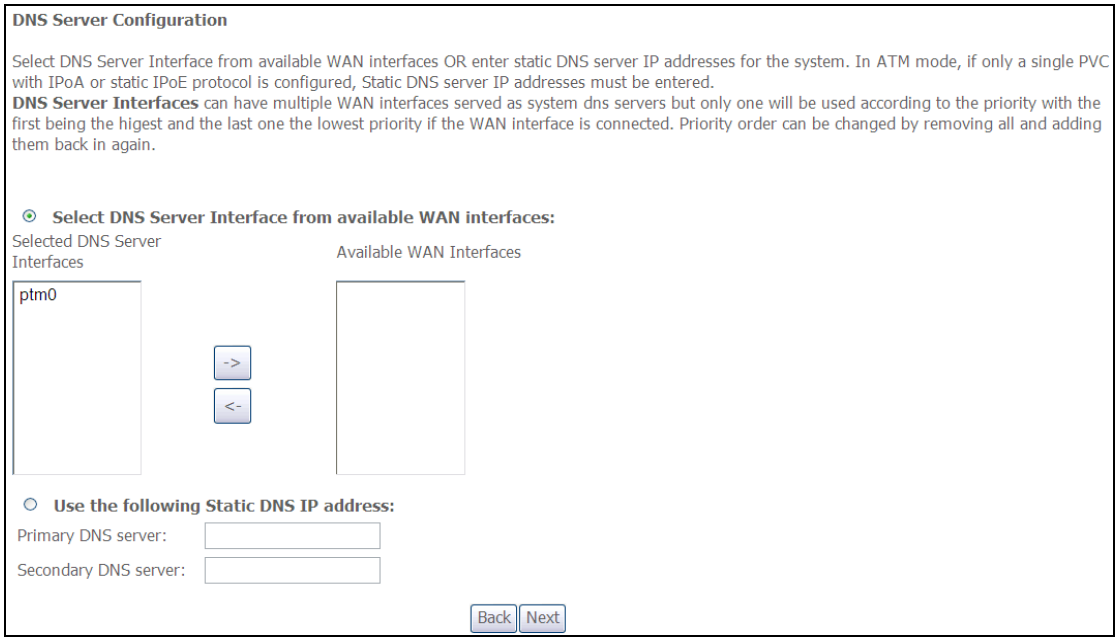
STEP 4: Choose an interface to be the default gateway.



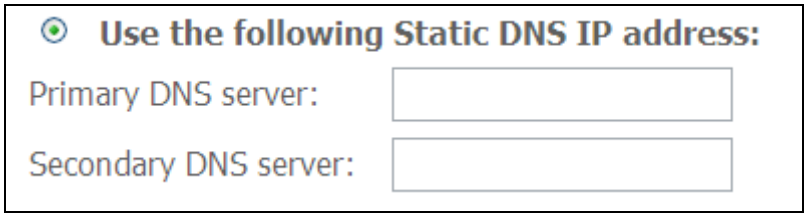
Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. Click **Next** to continue or click **Back** to return to the previous step.

Note: In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

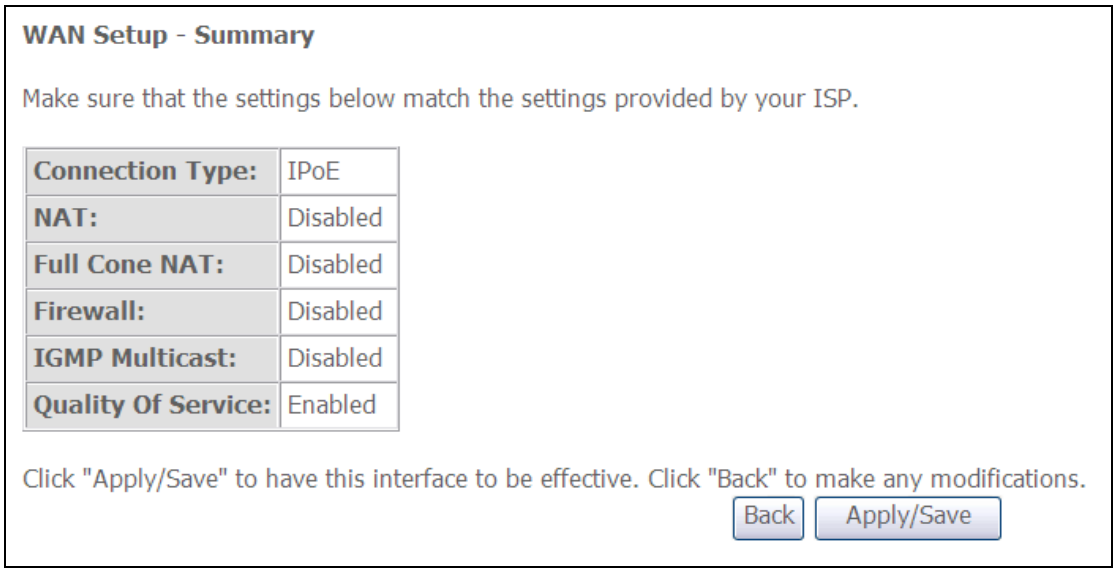


STEP 6: Set the IP address to which the CPE will use to relay DNS query.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 7: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.

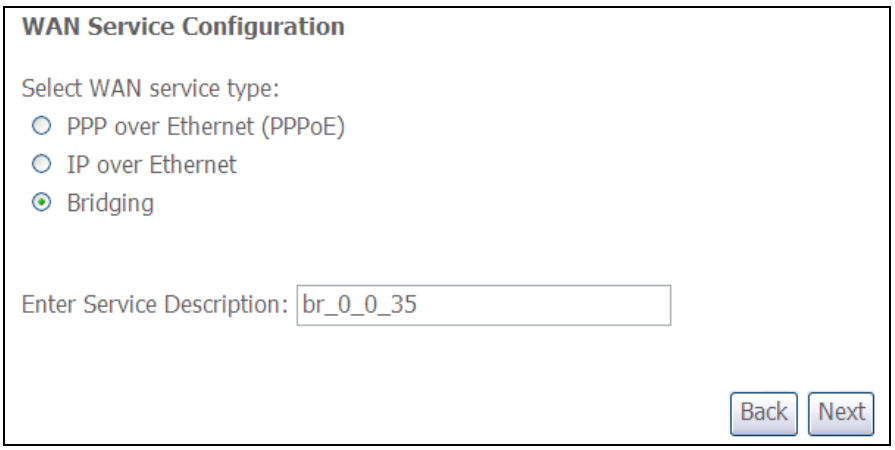


After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

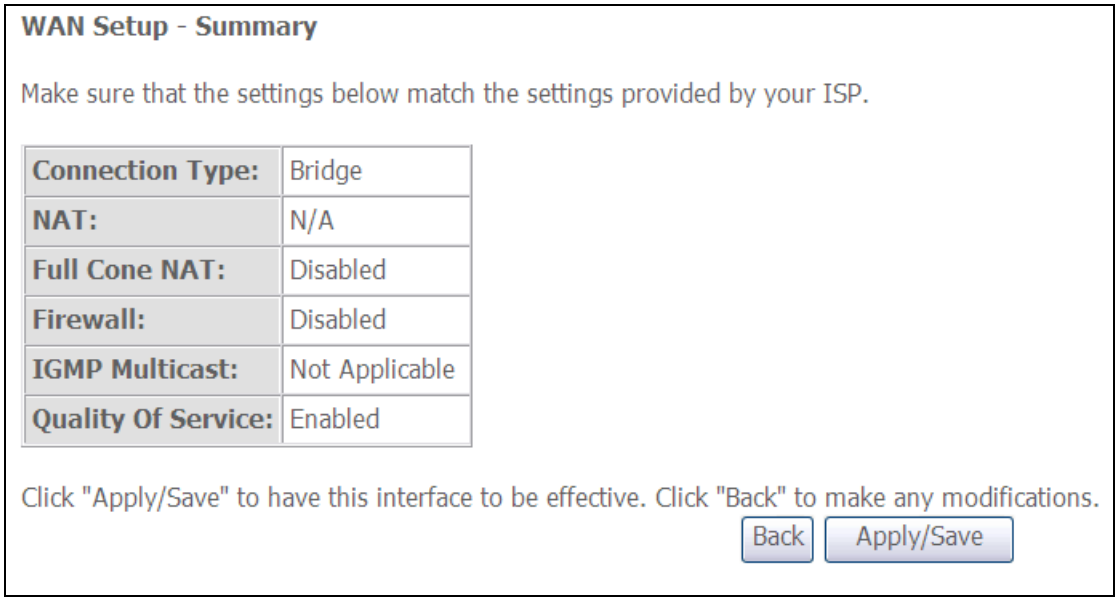
F2.3 Bridging

NOTE:	This connection type is not available on the Ethernet WAN interface.

STEP 1: Select the Bridging radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.



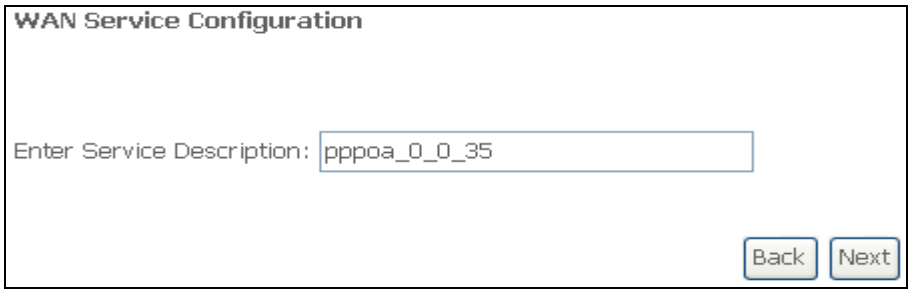
STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to return to the previous screen.



After clicking **Apply / Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

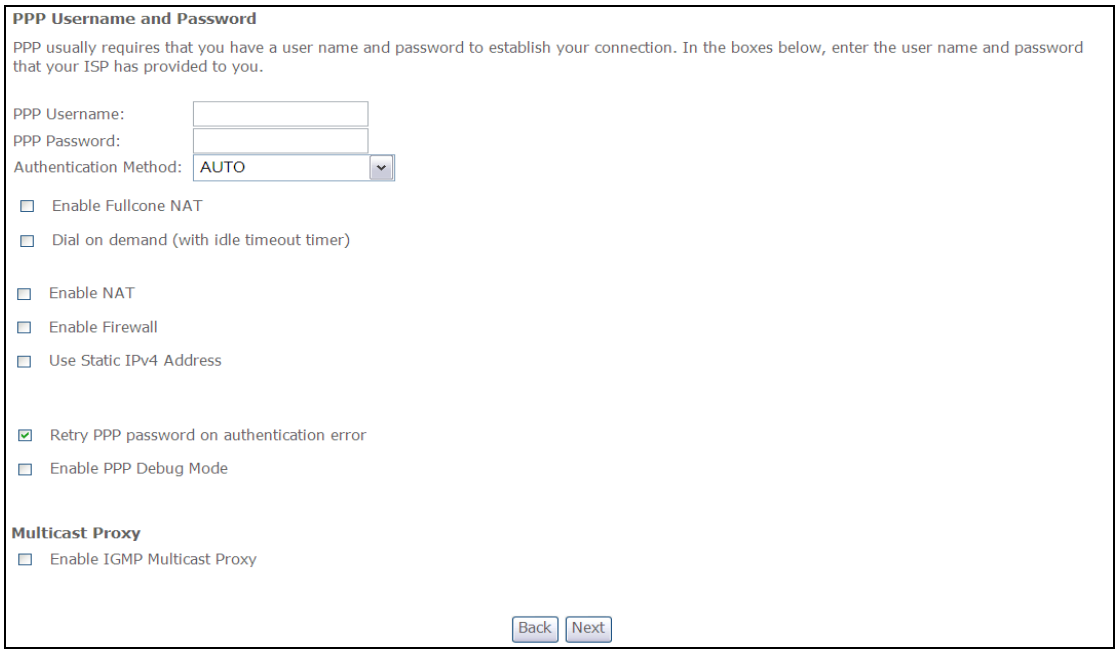
NOTE:	If this bridge connection is your only WAN service, the AR-5382u will be inaccessible for remote management or technical support from the WAN.

F2.4 PPP over ATM (PPPoA)



STEP 1: Click **Next** to continue.

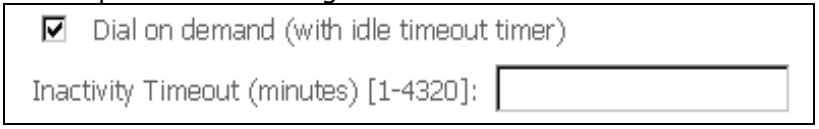
STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.



PPP SETTINGS
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The AR-5382u can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

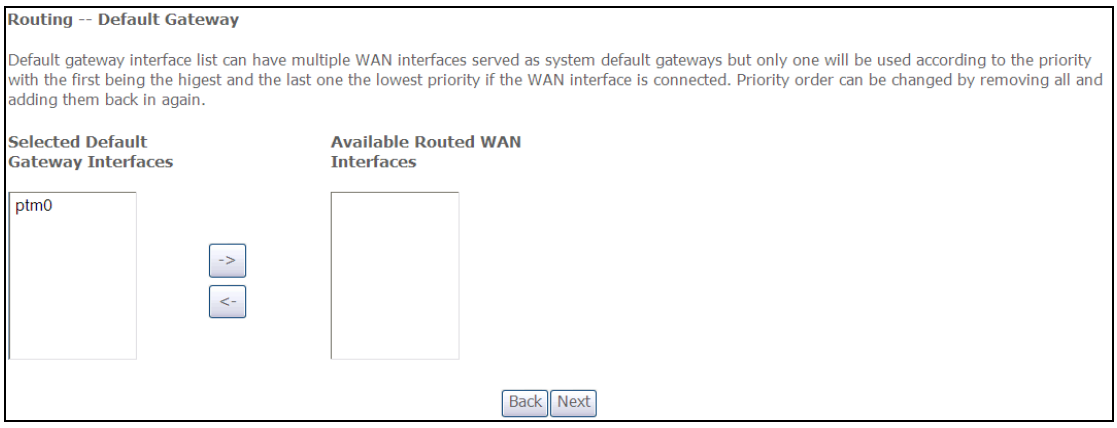
USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in 3.2 IP Configuration.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

Retry PPP password on authentication error
This feature will redirect users to another WEB page for PPP username/password re-entry if PPP authentication fails.
Tick the box to select.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

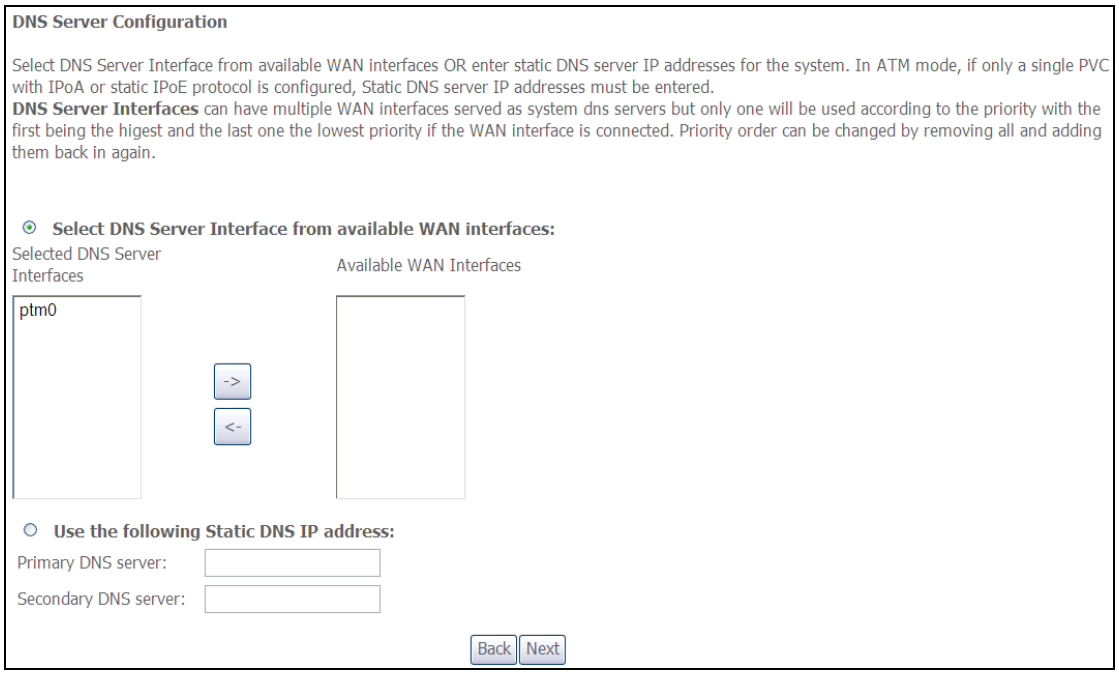
STEP3: Choose an interface to be the default gateway.



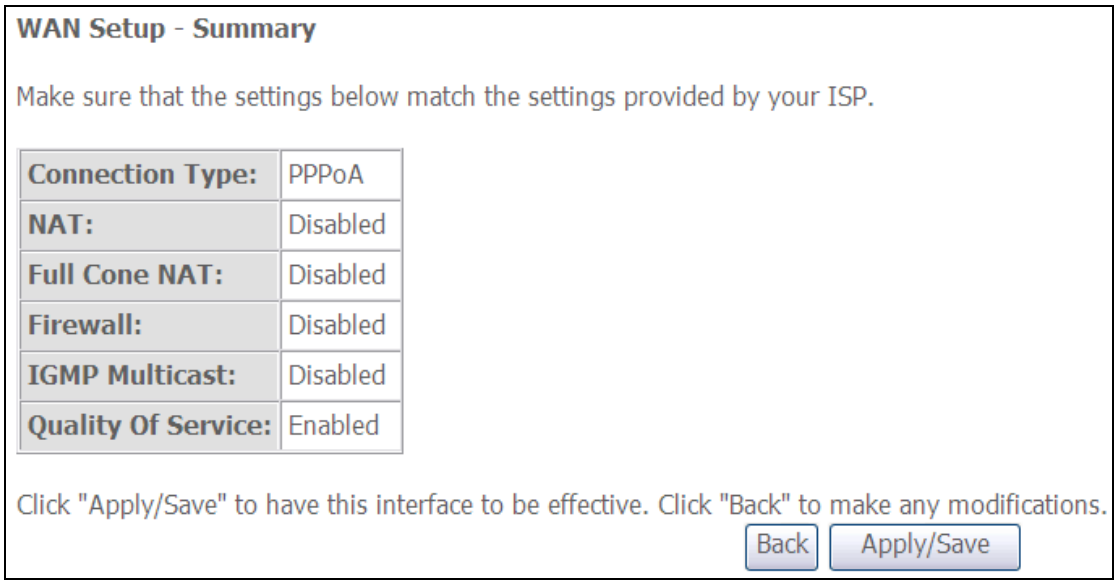
Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. Click **Next** to continue or click **Back** to return to the previous step.

Note: In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

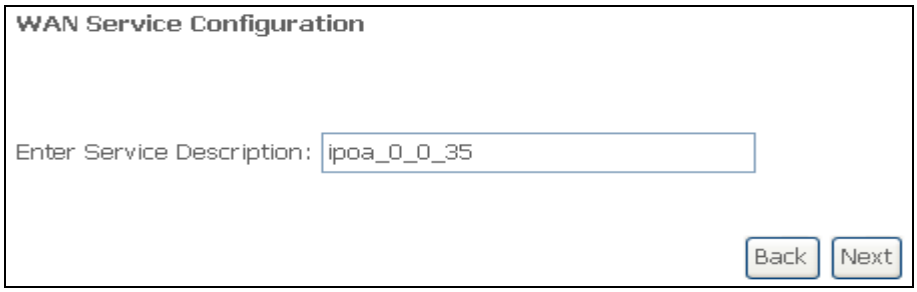


STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.



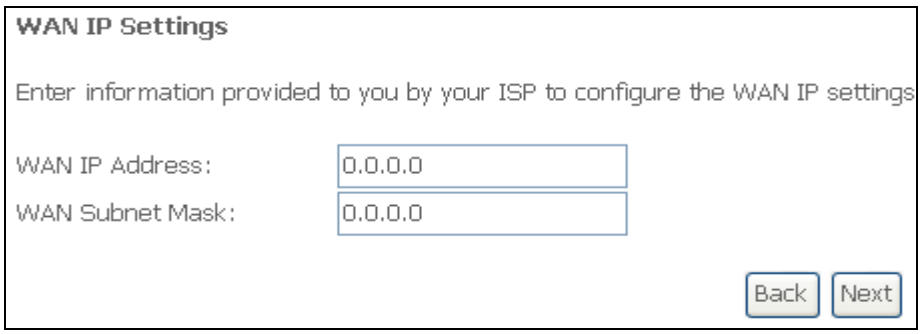
After clicking **Apply / Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

F2.5 IP over ATM (IPoA)

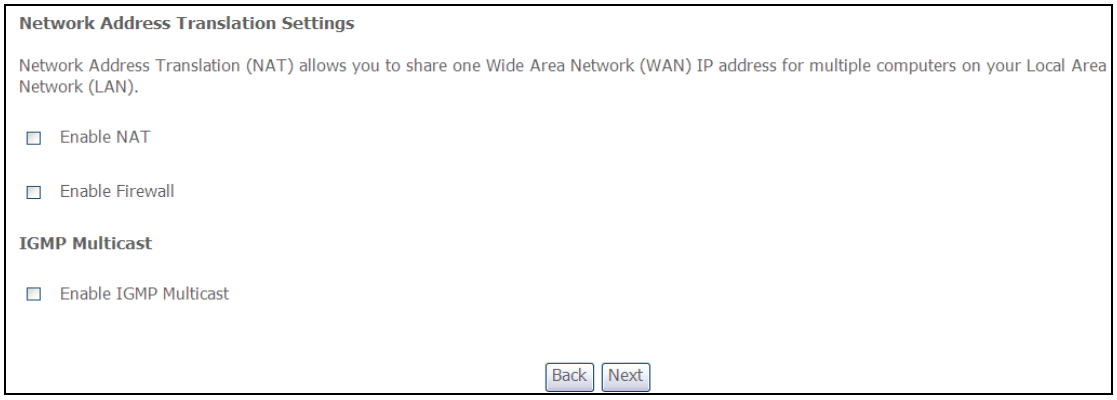


STEP 1: Click **Next** to continue.

STEP 2: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.



STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.

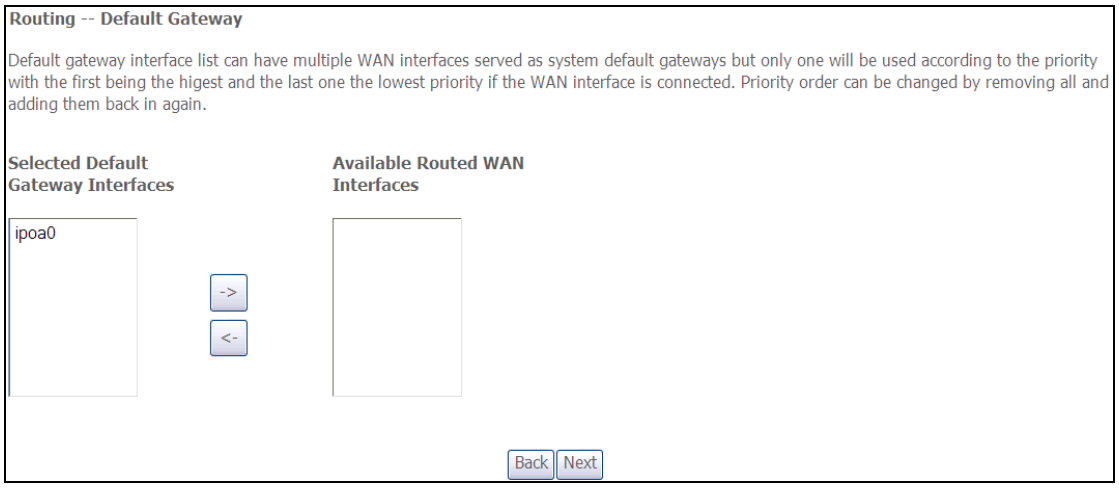


ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

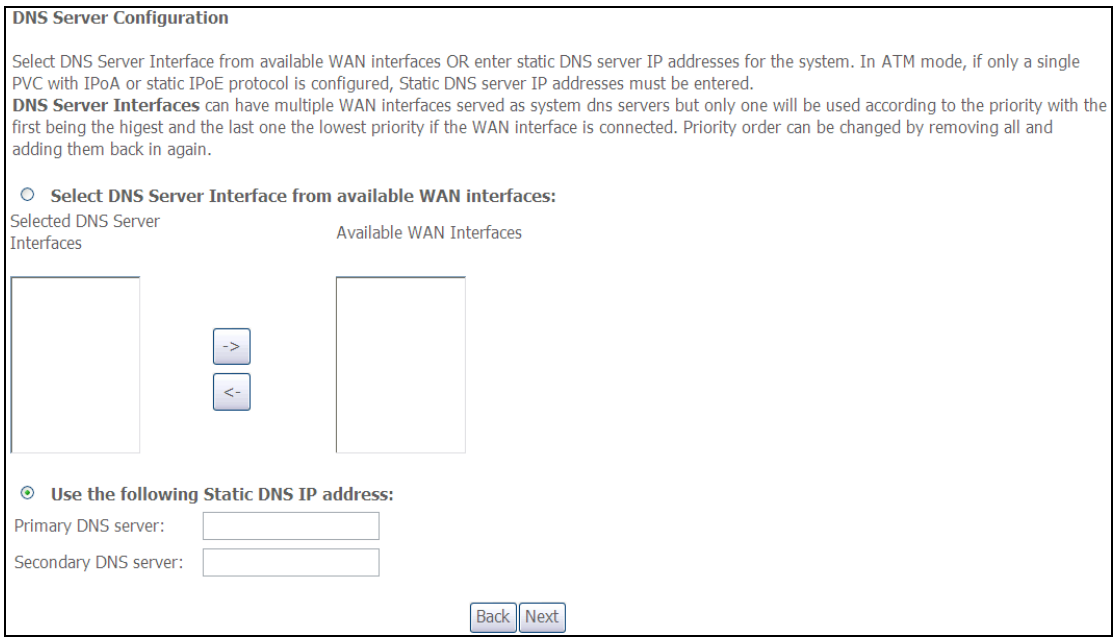
STEP4: Choose an interface to be the default gateway.



Click **Next** to continue or click **Back** to return to the previous step.

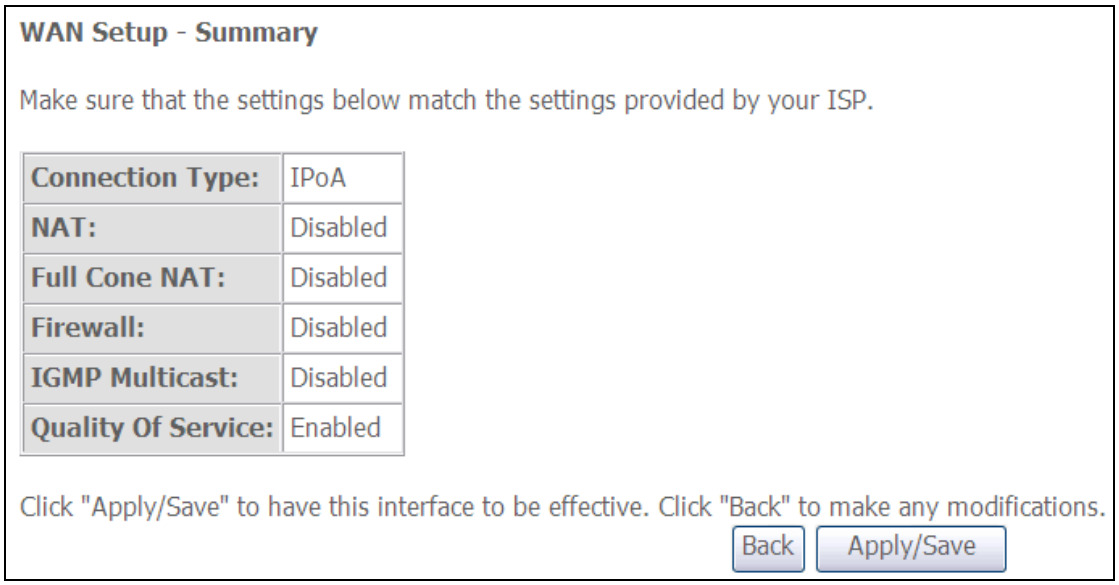
STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. Click **Next** to continue or click **Back** to return to the previous step.

Note: In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



NOTE: If the DHCP server is not enabled on another WAN interface then the following notification will be shown before the next screen.

STEP 7: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.



After clicking **Apply / Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.